Characterization of the type of Hopf-Galois structures on cyclic extensions

Cindy Tsang

Ochanomizu University (Japan)

Supported by JSPS KAKENHI 21K20319.

Hopf Algebras & Galois Module Theory

Online & University of Nebraska Omaha

May 30, 2022

The type of a Hopf-Galois structure

- Let L/K be a finite Galois extension with Galois group G.
- By Greither-Pareigis, there is a one-to-one correspondence between:
  1. Hopf-Galois structures on the Galois extension L/K
  2. regular subgroups in the symmetric group of the Galois group G which are normalized by the subgroup of left translations
- The type of a Hopf-Galois structure is defined to be the isomorphism class of the corresponding regular subgroup.
- These regular subgroups will have the same order as G. But not all groups of the same order as G will occur as a type of a Hopf-Galois structure.
- Question. For which groups N of the same order as G is there a Hopf-Galois structure H on L/K such that the type of H is the isomorphism class of N?
- If $N \simeq G$, then the answer is "yes". If $N \not\simeq G$, then it requires investigation.
- There is also the question of "how many" but I will focus on existence here.

Setting

- Cyclic groups have the simplest structure of all groups.
- It seems natural to consider finite cyclic extensions.
- This is the setting that I want to look at in this talk.

- Let L/K be a cyclic extension of degree n.
- Let N denote an arbitrary group of order n.
- Question. Is there a Hopf-Galois structure on L/K such that its type is the isomorphism class of N?
- Question. Is there a regular subgroup in $\mathrm{Perm}(G)$ which is normalized by left translations and is isomorphic to N?
- Ultimate Goal. Give a complete characterization of the N for which the answer to the above questions is yes.

Known results

Prime power degree

- Let L/K be a cyclic extension of prime power degree p^a.
- Let N denote an arbitrary group of order p^a.
- Question. Is there a Hopf-Galois structure on L/K such that its type is the isomorphism class of N?
- As in many other situations, the prime 2 exhibits a different behavior.
- (Kohl 1998). In the case that $p \geq 3$ ...
  - "yes" $\iff$ N is cyclic
- (Byott 1996 & 2007). In the case that $p = 2$ ...
  - "yes" $\iff$ N is cyclic, $\underbrace{\text{dihedral}}_{\text{when } a \geq 2}$, or $\underbrace{\text{quaternion}}_{\text{when } a \geq 3}$

$$D_{2^a} = \langle r, s \mid r^{2^{a-1}} = 1,\ s^2 = 1,\ srs^{-1} = r^{-1} \rangle \qquad (a \geq 2)$$

$$Q_{2^a} = \langle r, s \mid r^{2^{a-1}} = 1,\ s^2 = r^{2^{a-2}},\ srs^{-1} = r^{-1} \rangle \qquad (a \geq 3)$$

- Remark. In both cases, the exact number of Hopf-Galois structures is known.

Nilpotent groups

- Let L/K be a cyclic extension of degree n.
- Let N denote an arbitrary nilpotent group of order n.
- Question. Is there a Hopf-Galois structure on L/K such that its type is the isomorphism class of N?
- (Byott 2017). This reduces to the prime power case since it suffices to consider the Sylow p-subgroups N_p of N individually for each prime p.

$$\text{“yes”} \iff \begin{cases} N_p \text{ is cyclic for odd primes } p \\ N_2 \text{ is cyclic, } \underbrace{\text{dihedral}}_{\substack{\text{occurs only} \\ \text{when } v_2(n) \geq 2}}, \text{ or } \underbrace{\text{quaternion}}_{\substack{\text{occurs only} \\ \text{when } v_2(n) \geq 3}} \end{cases}$$

- Remark. Again, the exact number of Hopf-Galois structures is known. It is simply the product of the numbers of Hopf-Galois structures of type N_p on a cyclic extension of degree $p^{v_p(n)}$ over all primes p dividing n.

- Let L/K be a cyclic extension of degree n.
- Let N denote an arbitrary group of order n.
- Question. Is there a Hopf-Galois structure on L/K such that its type is the isomorphism class of N?
- For nilpotent groups N, this has been solved completely.
- Certainly the answer can be "yes" for non-nilpotent groups N.
- (Alabdali & Byott 2018). For n squarefree, the answer is "always yes".
- Remark. The exact number of Hopf-Galois structures is known. But if we only care about existence, then the answer being "always yes" may be explained by the fact that every group of squarefree order is a C-group.
- A C-group is a finite group in which all Sylow subgroups are cyclic.

C-groups

- Let L/K be a cyclic extension of degree n.
- Let N denote an arbitrary C-group of order n.
- Question. Is there a Hopf-Galois structure on L/K such that its type is the isomorphism class of N?
- (Known). The answer is "always yes".
- *Proof.* By Byott-Childs (2012), it suffices to show that there exists a pair of fixed point free homomorphisms $f, h : C_n \longrightarrow N$. By Murty-Murty (1984), every C-group is of a semidirect product $N = C_e \rtimes C_d$ with $\gcd(e, d) = 1$. But then $C_n = C_e \times C_d$ and clearly

$$f, h : C_e \times C_d \longrightarrow C_e \rtimes C_d; \quad \begin{cases} f(x, y) = (x, 1) \\ h(x, y) = (1, y) \end{cases}$$

define a pair of fixed point free homomorphisms. □

- Let L/K be a cyclic extension of degree n.
- Let N denote an arbitrary group of order n.
- Question. Is there a Hopf-Galois structure on L/K such that its type is the isomorphism class of N?
- For nilpotent groups N, this has been solved completely.
- For C-groups N, the answer is always yes.
- Certainly the answer can be "yes" for non-C-groups N.
- (Byott 1996 & 2007). For $n = 2^a$, we have

$$\text{"yes"} \iff N \text{ is cyclic, } \underbrace{\text{dihedral}}_{\text{when } a \geq 2}, \text{ or } \underbrace{\text{quaternion}}_{\text{when } a \geq 3}.$$

  Dihedral and quaternion groups are clearly not C-groups.

- Thus, that N being a C-group is only sufficient but not necessary.

Supersolvability

- Let L/K be a cyclic extension of degree n.
- Let N denote an arbitrary group of order n.
- Question. Is there a Hopf-Galois structure on L/K such that its type is the isomorphism class of N?
- A supersolvable group is a group which admits a normal series such that each quotient group in the series is cyclic.
- For example, all C-groups are supersolvable groups.
- (T. 2020). The answer is "yes" only if N is supersolvable.
- Unfortunately N being supersolvable is only necessary but not sufficient.
- The N's that can occur lie somewhere between C-group and supersolvable.

New results

Preliminary restriction

- Let L/K be a cyclic extension of degree n.
- Let N denote an arbitrary group of order n.
- Question. Is there a Hopf-Galois structure on L/K such that its type is the isomorphism class of N?

Proposition (T., arXiv:2107.1369)

The answer is "yes" only if $N = M \rtimes P$, where M is a C-group of odd order and P is a possibly trivial cyclic, dihedral, or quaternion group of order a power of 2.

- *Proof (Sketch).* We may assume that N is supersolvable, in which case

$$N = M \rtimes P, \text{ where } P \text{ is a Sylow 2-subgroup of } N$$

- the M part: reduces to the prime power case by induction on the number of prime divisors
- the P part: reduces to the 2-power case
- One then obtains the proposition from previously known results. □
- Unfortunately this condition is also only necessary but not sufficient.

Some calculations

- Take $n = 84$ and note that $n = 21 \cdot 4$.
- M can be the cyclic group C_{21} or the non-abelian group $C_7 \rtimes C_3$.
- P can be the cyclic group C_4 or the elementary abelian group D_4, and we may ignore the cyclic group C_4 for otherwise N is a C-group.
- There are seven candidates for $N = M \rtimes_\alpha P$. By computing the cyclic regular subgroups in the holomorph of N using MAGMA, I found that ...

1. $\textsc{SmallGroup}(84, 8)$: $N = C_{21} \rtimes_{\alpha_1} D_4$ answer is "no"
2. $\textsc{SmallGroup}(84, 12)$: $N = C_{21} \rtimes_{\alpha_2} D_4$ answer is "yes"
3. $\textsc{SmallGroup}(84, 13)$: $N = C_{21} \rtimes_{\alpha_3} D_4$ answer is "yes"
4. $\textsc{SmallGroup}(84, 14)$: $N = C_{21} \rtimes_{\alpha_4} D_4$ answer is "yes"
5. $\textsc{SmallGroup}(84, 15)$: $N = C_{21} \rtimes_{\alpha_5} D_4$ answer is "yes"
6. $\textsc{SmallGroup}(84, 7)$: $N = (C_7 \rtimes C_3) \rtimes_{\alpha_6} D_4$ answer is "yes"
7. $\textsc{SmallGroup}(84, 9)$: $N = (C_7 \rtimes C_3) \rtimes_{\alpha_7} D_4$ answer is "yes"

Main theorem

- Let L/K be a cyclic extension of degree n.
- Let N denote an arbitrary non-C-group of order n.
- Question. Is there a Hopf-Galois structure on L/K such that its type is the isomorphism class of N?

Theorem (T., arXiv:2107.1369)

The answer is "yes" if only if $N \simeq M \rtimes_\alpha P$, where M is a C-group of odd order, P is a dihedral or quaternion group of order a power of 2, and α satisfies

a. $\alpha(P)$ has order 1 or 2 when $P = D_4$ or $P = Q_8$;
b. $\alpha(r) = \mathrm{Id}_M$ when $P = D_{2^a}$ with $a \geq 3$ or $P = Q_{2^a}$ with $a \geq 4$.

Here r is the generator in the usual presentation of dihedral or quaternion groups.

- Reason for the difference. There exist $\kappa_1, \kappa_2 \in \mathrm{Aut}(P)$ for which $\kappa_1(r) = s$ and $\kappa_2(r) = rs$ in case (a), while $\langle r \rangle$ is a characteristic subgroup in case (b).

Explanation for the calculations

- The answer is "yes" if and only if $\alpha_i(D_4)$ has order 1 or 2.

1. $\textsc{SmallGroup}(84, 8)$: $N = C_{21} \rtimes_{\alpha_1} D_4$ answer is "no"
2. $\textsc{SmallGroup}(84, 12)$: $N = C_{21} \rtimes_{\alpha_2} D_4$ answer is "yes"
3. $\textsc{SmallGroup}(84, 13)$: $N = C_{21} \rtimes_{\alpha_3} D_4$ answer is "yes"
4. $\textsc{SmallGroup}(84, 14)$: $N = C_{21} \rtimes_{\alpha_4} D_4$ answer is "yes"
5. $\textsc{SmallGroup}(84, 15)$: $N = C_{21} \rtimes_{\alpha_5} D_4$ answer is "yes"
6. $\textsc{SmallGroup}(84, 7)$: $N = (C_7 \rtimes C_3) \rtimes_{\alpha_6} D_4$ answer is "yes"
7. $\textsc{SmallGroup}(84, 9)$: $N = (C_7 \rtimes C_3) \rtimes_{\alpha_7} D_4$ answer is "yes"

- $\mathrm{Aut}(C_{21}) \simeq C_6 \times C_2$ has Sylow 2-subgroup $\simeq D_4$.
  - $\underbrace{\alpha_1(D_4) \simeq D_4}_{\text{no}}, \underbrace{\alpha_2(D_4), \alpha_3(D_4), \alpha_4(D_4) \simeq C_2, \alpha_5(D_4) \simeq C_1}_{\text{yes}}$
- $\mathrm{Aut}(C_7 \rtimes C_3) \simeq C_7 \rtimes C_6$ has Sylow 2-subgroup $\simeq C_2$.
  - $\underbrace{\alpha_6(D_4) \simeq C_2, \alpha_7(D_4) \simeq C_1}_{\text{yes}}$

Thank you for listening!