Hopf-Galois structures on non-normal extensions of degree related to a Sophie Germain prime

Nigel Byott

University of Exeter

Omaha (virtually), 24 May 2021

(Joint work with Isabel Martin-Lyons and Andrew Darlington)

Outline

§1: A Quick Review of Hopf-Galois Theory

Let L/K be a finite extension of fields of degree n. A **Hopf-Galois Structure** (HGS) on L/K consists of a cocommutative Hopf algebra H over K, and an action of H on L so that

- $$h \cdot (xy) = \sum_{(h)} (h_{(1)} \cdot x)(h_{(2)} \cdot y) \text{ for } h \in H \text{ and } x, y \in L,$$

  where we write the comultiplication $\Delta : H \to H \otimes_K H$ as $h \mapsto \sum_{(h)} h_{(1)} \otimes h_{(2)}$;
- $h \cdot k = \epsilon(h)k$ for $h \in H$ and $k \in K$.
- K-linear map $\theta : L \otimes_K H \to \mathrm{End}_K(L)$ given by $\theta(x \otimes h)(y) = x(h \cdot y)$ is bijective.

For example, if L/K is a Galois (normal and separable) extension, we can take $H = K[G]$ for $G = \mathrm{Gal}(L/K)$.

When L/K is separable, Greither and Pareigis (1987) described all Hopf-Galois structures. Let

- E/K be the normal closure of L/K,
- $G = \mathrm{Gal}(E/K)$,
- $G' = \mathrm{Gal}(E/L)$,
- $X = G/G'$, the space of left cosets.

Then Hopf-Galois structures on L/K correspond bijectively to regular subgroups $N \subset \mathrm{Perm}(X)$ which are normalised by the group $\lambda(G)$ of left translations by G.

So the group N has order n. We call the isomorphism type of N the **type** of the corresponding HGS.

We say this HGS is *almost classically Galois* if N has a normal complement in G.

§1.1: The Galois Case

When L/K is a Galois extension, $X = G = \mathrm{Gal}(L/K)$ and we have two groups N and G of order n in the picture. This situation has been investigated for many Galois groups G.

Regular *embeddings* of an abstract group N into $\mathrm{Perm}(G)$ with image normalised by $\lambda(G)$ correspond to regular *embeddings* of G of the holomorph $\mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N)$ of N. This gives a counting formula

$$\begin{aligned} &\#\{\text{HGS of type } N \text{ on } L/K\} \\ &\quad = \quad \frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(N)|} \times \#\{\text{regular subgroups of } \mathrm{Hol}(N) \text{ isomorphic to } G\}. \end{aligned}$$

Regular embeddings $G \to \mathrm{Hol}(N)$ are also related to skew braces with additive group N and multiplicative group G, so studying Hopf-Galois structures on finite Galois extensions of fields is in some sense equivalent to studying skew braces.

§1.2: The Non-Galois Case

The situation where L/K is not normal (but still separable) has not been as thoroughly investigated (and there is no direct interpretation in terms of skew braces), but some results are known.

Recall $n = [L : K]$, E/K is the normal closure of L/K, $G = \mathrm{Gal}(E/K)$, $G' = \mathrm{Gal}(E/L)$.

- (Childs, 1989): If $n = p$ is prime, L/K admits a HGS $\Leftrightarrow$ G is soluble (so $G \leq C_p \rtimes C_{p-1}$).
- Kohl (1998) studied HGS on extensions of the form $K(\sqrt[p^n]{a})/K$ for odd primes p.
- Crespo and Salguero (2020) gave theoretical and computational results for degrees p^2 and $2p$.

In the non-normal case, G acts as a transitive permutation group (of *degree* n) on the coset space $X = G/G'$, and the choice of E ensures that

$$\mathrm{Core}_G(G') := \bigcap_{g \in G} gG'g^{-1} = \{1\}.$$

We can think of a transitive permutation group of degree n abstractly as a pair (G, G') consisting of a group G and a (conjugacy class of) subgroup(s) G' of index n with $\mathrm{Core}_G(G') = \{1\}$.

The counting formula still works in the non-normal case if we replace $\mathrm{Aut}(G)$ by

$$\mathrm{Aut}(G, G') = \{\theta \in \mathrm{Aut}(G) : \theta(G') = G'\}$$

the automorphisms of G as a permutation group (with fixed base point, i.e. the coset $1_G G'$).

§2: Extensions of squarefree degree

Let n be squarefree. Then there is a classification of groups of order n. (They are all metacyclic.) If we pick any two groups N and G of order n, we can count the HGS (if any) of type N on a Galois extension with Galois group G (Alabdali+B, 2020) and also the corresponding skew braces (Alabdali + B; 2021).

Question: Can we count HGS for non-normal extensions of degree n for (at least some) squarefree n?

Any such HGS has a type N (a group of order n in our classification) and and associated permutation group (G, G') of degree n. As $|G|$ is usually *not* squarefree, we have no classification of these permutation groups.

So our Question looks hopeless. But ...

...most of the permutation groups of degree n are irrelevant for Hopf-Galois theory.

e.g., for $n = p$ (prime), we know that amongst all the transitive subgroups of S_p, only those in $C_p \rtimes C_{p-1}$ are relevant.

This suggests the following strategy (given a squarefree n):

1. For each group N of order n (up to isomorphism), find all transitive subgroups $G \leq \mathrm{Hol}(N)$. These give permutation groups (G, G') of degree n, where G' is the stabiliser of 1_N.
2. Determine which pairs of permutation groups

$$(G_1, G_1') \leq \mathrm{Hol}(N_1) \text{ and } (G_2, G_2') \leq \mathrm{Hol}(N_2)$$

(where N_1, N_2 are possibly different groups of order n) are isomorphic as permutation groups.

If there is a such an isomorphism of permutation groups (with $N_1 \ncong N_2$), then the corresponding field extensions will admit Hopf-Galois structures of type N_1 and of type N_2.

This strategy will not find all permutation groups of degree n, but it will find those that are relevant to Hopf-Galois Theory. In fact, if N has squarefree order then both N and $\mathrm{Aut}(N)$ are metabelian, so any $G \leq \mathrm{Hol}(N)$ is soluble with derived length ≤ 4.

§3: The "Sophie Germain" Case

We consider squarefree numbers of a very special form:

$$n = pq$$

where $q \geq 3$ is prime and $p = 2q + 1$ is also prime. (So q is a Sophie Germain prime, and p is a safeprime.)

This case was investigated in an LMS-funded summer research project (2019): see (B+Martin-Lyons, arXiv).

There are two groups N to consider

- the cyclic group $N = C_p \times C_q$, with $\mathrm{Aut}(N) \cong C_{2q} \times C_{q-1}$;
- the metabelian group $N = C_p \rtimes C_q$, with $\mathrm{Aut}(N) \cong C_p \rtimes C_{2q}$.

Write $q - 1 = 2^r s$ with $r \geq 1$, s odd.

(i) For $N = C_p \times C_q$, we have $|\mathrm{Hol}(N)| = 2^{r+1}pq^2s$.

The Sylow 2-subgroup of $\mathrm{Hol}(N)$ has the form $C_2 \times C_{2^r}$.

For a transitive subgroup $G \leq \mathrm{Hol}(N)$, let 2^c be the exponent of its Sylow 2-subgroup, and let $d = \gcd(|H|, s)$. The number of possibilities for d is $\sigma_0(s)$, the number of divisors of s.

G must also contain either N itself or one of a family of $q-1$ regular metabelian subgroups J_t, $1 \leq t \leq q-1$.

We can then list the possible groups G.

Key	Restrictions	Order	Structure
(A)	$(c,d) \neq (0,1), (1,1)$	$2^{c+1}pq^2d$	$(C_p \rtimes C_{2q}) \times (C_q \rtimes C_{2^c d})$
	$(c,d) = (1,1)$	$4pq^2$	$(C_p \rtimes C_{2q}) \times D_{2q}$
	$(c,d) = (0,1)$	$2pq^2$	$(C_p \rtimes C_{2q}) \times C_q$
(B)	$(c,d) \neq (0,1), (1,1)$	$2^c pq^2 d$	$(C_p \rtimes C_q) \times (C_q \rtimes C_{2^c d})$
	$(c,d) = (1,1)$	$2pq^2$	$(C_p \rtimes C_q) \times D_{2q}$
	$(c,d) = (0,1)$	pq^2	$(C_p \rtimes C_q) \times C_q$
(C)		$2^c pq^2 d$	$C_{pq} \rtimes C_{2^c dq}$
(D)	$(c,d) \neq (0,1), (1,1)$	$2^{c+1}pqd$	$D_{2p} \times (C_q \rtimes C_{2^c d})$
	$(c,d) = (1,1)$	$4pq$	$D_{2p} \times D_{2q}$
	$(c,d) = (0,1)$	$2pq$	$D_{2p} \times C_q$
(E)	$(c,d) \neq (0,1), (1,1)$	$2^c pqd$	$C_p \times (C_q \rtimes C_{2^c d})$
	$(c,d) = (1,1)$	$2pq$	$C_p \times D_{2q}$
	$(c,d) = (0,1)$	pq	$C_{pq} = N$
(F)	$(c,d) \neq (1,1)$	$2^c pqd$	$C_{pq} \rtimes C_{2^c d}$
	$(c,d) = (1,1)$	$2pq$	D_{2pq}
(G)		$2pq$	$C_p \rtimes C_{2q}$ $(q-1$ groups$)$
(H)		pq	$C_p \rtimes C_q$ $(q-1$ groups$)$

The $q-1$ groups (G) of order $2pq$ are isomorphic, and the $q-1$ groups (H) of order pq (i.e. the groups J_t) are isomorphic. There are no other isomorphisms (of abstract groups or of permutation groups). From the table, we deduce

Theorem

There are in total $(6r+4)\sigma_0(s)+2$ *isomorphism types of permutation groups* G *of degree* pq *which are realised by a Hopf-Galois structure of cyclic type.*

These include the two regular groups, i.e. the cyclic and non-abelian groups of order pq*.*

[There is one cyclic regular subgroup of $\mathrm{Hol}(N)$*, corresponding to the unique (classical) HGS of cyclic type on a cyclic extension of degree* n*, and* $q-1$ *metabelian subgroups, corresponding to the* p *HGS of cyclic type on a metabelian extension of degree* n*.]*

For all the remaining groups G*, any field extension* L/K *realising* G *is almost classically Galois and admits a unique Hopf-Galois structure of cyclic type.*

(ii) Now let N be the metabelian group. Then $|\mathrm{Hol}(N)| = 2p^2q^2$.

By definition, $\mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N)$, but there is another semidirect product decomposition

$$\mathrm{Hol}(N) = P \rtimes R,$$

where $P \cong C_p \times C_p = \mathbb{F}_p^2$, and $R \cong C_2 \times C_q \times C_q$ can be identified with a group of diagonal matrices in $\mathrm{GL}_2(\mathbb{F}_p)$. (Recall $q = (p-1)/2$.)

We can use this to find the subgroups of $\mathrm{Hol}(N)$ which are transitive *on* N.

Order	Structure	# groups	# HGS
p^2q^2	$N \rtimes (C_p \rtimes C_q)$	1	2
$2p^2q^2$	$\mathrm{Hol}(N)$	1	2
p^2q	$C_p \times (C_p \rtimes C_q)$	2	$2p$
	$\mathbb{F}_p^2 \rtimes_u C_q$, $1 \leq u \leq \frac{1}{2}(q-3)$	2	$2p$
	$\mathbb{F}_p^2 \rtimes_{\frac{1}{2}(q-1)} C_q$	1	$2p$
$2p^2q$	$(C_p \times (C_p \rtimes C_q)) \rtimes C_2$	2	$2p$
	$\mathbb{F}_p^2 \rtimes_u C_{2q}$, $1 \leq u \leq \frac{1}{2}(q-3)$	2	$2p$
	$\mathbb{F}_p^2 \rtimes_{\frac{1}{2}(q-1)} C_{2q}$	1	$2p$
pq^2	$C_q \times (C_p \rtimes C_q)$	$2p$	$2(q-1)$
$2pq^2$	$C_q \times (C_p \rtimes C_{2q})$	$2p$	$2(q-1)$
pq	$C_p \rtimes C_q$	$2p(q-2)+2$	$2p(q-2)+2$
	C_{pq}	$2p$	$2(q-1)$
$2pq$	$C_p \rtimes C_{2q}$	$2p(q-1)$	$2(q-1)$
	$D_{2p} \times C_q$	$2p$	$2(q-1)$

Theorem

There are in total $q+9$ isomorphism types of permutation groups G of degree pq which are realised by Hopf-Galois structures of non-abelian type $C_p \rtimes C_q$, as listed in the previous table.

These include the two regular groups, i.e. the cyclic and non-abelian groups of order pq (for which the corresponding Galois extensions have $2(q-1)$ and $2p(q-2)+2$ Hopf-Galois structures of non-abelian type respectively).

For $q-1$ of these permutation groups (i.e. all but one of each of the orders p^2q, $2p^2q$), the corresponding field extensions fail to be almost classically Galois. In the remaining 10 cases, the extensions are almost classically Galois.

We can also pick out the cases where there are Hopf-Galois structrures of both types. There are 6 such groups G.

Order	Structure	# cyclic type HGS	# non-abelian type HGS
$2pq^2$	$C_q \times (C_p \rtimes C_{2q})$	1	$2(q-1)$
pq^2	$C_q \times (C_p \rtimes C_q)$	1	$2(q-1)$
$2pq$	$C_p \rtimes C_{2q}$	1	$2(q-1)$
$2pq$	$D_{2p} \times C_q$	1	$2(q-1)$
pq	$C_p \rtimes C_q$	p	$2p(q-2)+2$
pq	C_{pq}	1	$2(q-1)$

In all these cases, the extensions are almost classically Galois.

(The last two rows give the *Galois* extensions of degree n, where the HGS were already known.)

§4: Other Degree n Extensions in the Normal Closure

As usual, let L/K be a separable extension, with normal closure E, and let $G = \mathrm{Gal}(E/K)$, $G' = Gal(E/L)$.

Let $n = [L : K]$ (not necessarily squarefree) and suppose that L/K admits a HGS of type N.

What can we say about other degree n subextensions of E/K?

By classical Galois theory, these are the fields $F = E^H$ as H runs through all subgroups of G of index n.

A priori, there are several possibilities:

- H is conjugate to G', so that F is a conjugate field to L. This is uninteresting!
- H is not conjugate to G', but there is some (outer) automorphism θ of G with $\theta(G') = H$. Then the permutation groups (G, G') and (G, H) are isomorphism, and L, F belong to different G-orbits of fields which "look the same" for Hopf-Galois theory. This is slightly more interesting!

- There is no automorphism of G taking G' to H, but still $\mathrm{Core}_G(H) = \{1\}$. Then F (like L) has normal closure E, and the permutation groups (G, G') and (G, H) are not isomorphic (despite having the same underlying group G).

  Then H and G' might or might not be isomorphic as abstract groups.

  If F/K admits a HGS, then (G, H) will show up as a transitive subgroup of $\mathrm{Hol}(N)$ or of $\mathrm{Hol}(M)$ for some other M of order n.

  Is it possible that F/K does *not* admit any HGS? That would be very interesting!

- If $C := \mathrm{Core}_G(H) \neq \{1\}$, then F would have a smaller normal closure E^C and would give a smaller permutation group $(G/C, H/C)$. Again, this permutation group might show up in some $\mathrm{Hol}(M)$, or F/K might not admit any HGS.

  (In the extreme case, $C = H$, we have that F/K is normal of degree n.)

In the Sophie Germain case ($n = pq$, q and $p = 2q + 1$ odd primes), Andrew Darlington (work in progress) has investigated the index n subgroups H in all the groups G arising as the Galois group of (the normal closure of) a degree n extension admitting a HGS.

For many of the groups G, we have $\gcd(n, |G|/n) = 1$. Since G is soluble, this automatically means all subgroups of index n are conjugate, by a theorem of Hall.

But, for example, when $N = C_p \rtimes C_q$ and G is the full group $\mathrm{Hol}(N)$ of order $2p^2q^2$, all the subgroups of index n are isomorphic to $C_p \rtimes C_{2q}$ (with C_{2q} acting faithfully).

- The index n subgroups with trivial core form 2 conjugacy classes of size pq and q conjugacy classes of size p. (So there are extensions L/K, F/K of degree n, with the same normal closure E, $\mathrm{Gal}(E/K) = G$, which "look different" for Hopf-Galois theory).
- There are also $2q + 2$ conjugacy classes of size p of groups of index n with core of order p. These correspond to non-normal degree n subfields $F \subset E$ whose normal closure is smaller than E. The extensions F/K do all admit Hopf-Galois structures.

In the Sophie Germain case, every degree n subfield of E does admit a HGS: we don't find any "very interesting" cases!

§5: Beyond Sophie Germain?

Given primes $p > q > 2$ with $p \mid (q-1)$, there are again two groups $C_p \times C_q$, $C_p \rtimes C_q$ of order $n = pq$.

Preliminary work by Andrew Darlington suggests that we can again carry out our strategy and determine all possible Hopf-Galois structures on degree n extensions. The main difference from the Sophie Germain case is that there may now be several primes ℓ dividing both $p-1$ and $q-1$, and so many possibilities for the Sylow ℓ-subgroup of $G \leq \mathrm{Hol}(C_p \times C_q)$.

Again, if L/K is a degree n extension admitting an HGS, and E/K is its normal closure, then every degree n subextension of E/K admits at least one HGS.

So again, the "very interesting" situation does not arise.

Thank you for listening!