Nilpotent (and soluble?) Hopf Galois Structures

Nigel Byott

University of Exeter, UK

Omaha, 29 May 2013

Hopf-Galois Structures

Let L/K be a finite Galois extension of fields, with $\Gamma = \mathrm{Gal}(L/K)$.

A *Hopf-Galois structure* on L/K consists of a Hopf algebra H over K and a "nice" K-linear action of H on L (basic example: $H = K[\Gamma]$):

- the action is compatible with the multiplication on N:

$$\alpha \cdot (xy) = \mathrm{mult}\left(\Delta(\alpha) \cdot (x \otimes y)\right),$$

$$\alpha \cdot 1 = \epsilon(\alpha)1 \text{ for all } \alpha \in K[G],\ x, y \in L,$$

  where Δ is the comultiplication and ϵ the augmentation;
- ("Galois", i.e. non-degeneracy, condition): the following map is bijective:

$$\theta : L \otimes_K H \longrightarrow \mathrm{End}_K L, \quad \theta(x \otimes h)(y) = x(h \cdot y).$$

In particular, this means $\dim_K H = [L : K]$ and H acts faithfully on L.

Classifying Hopf Galois Structures

Greither and Pareigis (1987) showed the Hopf Galois structures correspond bijectively to subgroups G of the (large) group $\mathrm{Perm}(\Gamma)$ which are **regular** (i.e. given $x, y \in \Gamma$ there is a unique $g \in G$ with $g \cdot x = y$) and are normalised by $\lambda(\Gamma)$, the left translations by Γ.

We can turn around the relation between Γ and G:

Hopf Galois structures correspond to equivalence classes of regular embeddings

$$\Gamma \longrightarrow \mathrm{Hol}(G) \subseteq \mathrm{Perm}(G),$$

where G is an abstract group with $|G| = |\Gamma|$, and

$$\mathrm{Hol}(G) = \{(g, \alpha) \mid g \in G,\ \alpha \in \mathrm{Aut}(G)\},$$

with $(g, \alpha)(h, \beta) = (g\alpha(h), \alpha\beta)$, i.e.

$$\mathrm{Hol}(G) = \lambda(G) \rtimes \mathrm{Aut}(G).$$

Two embeddings are deemed to be equivalent if they are conjugate by an element of $\mathrm{Aut}(G)$.

The **type** of the HGS is (the isomorphism class of) G.

We can use this to count the HGS on a field extension L/K with given Galois group Γ.

Example: Cyclic Extensions of Prime-Power Degree

For $\Gamma = C_{p^r}$ with p an odd prime, there are p^{r-1} Hopf Galois structures, all with $G = C_{p^r}$ [Kohl].

The case $p = 2$ is more complicated: for $\Gamma = C_{2^r}$,

- if $r = 1$, there is one Hopf Galois structure, with $G = C_2$;
- if $r = 2$, there is one Hopf Galois structure with $G = C_4$ and one with $G = C_2 \times C_2$;
- if $r \geq 3$, there are $3 \cdot 2^{r-2}$ Hopf Galois structures, 2^{r-2} each for $G = C_{2^r}, Q_{2^r}, D_{2^r}$.

Non-abelian HGS on abelian extensions

"Most" abelian Γ admit a non-abelian HGS.

Theorem (L. Childs + NB)

Let Γ be an abelian group of order n. Then a Galois field extension with group Γ admits a non-abelian HGS if any of the following hold:

(i) *Γ contains a non-cyclic p-subgroup of order $\geq p^3$;*

(ii) *n is even and $n > 4$;*

(iii)
$$\Gamma = \prod_{p \in \Theta} (C_p \times C_p) \times \prod_{p \in \Psi} C_{p^{e_p}},$$
where Θ, Ψ are disjoint sets of primes, and either

- (a) $(q, p-1) > 1$ *for some* $p, q \in \Theta \cup \Psi$, *or*
- (b) $(q, p+1) > 1$ *for some* $p \in \Theta$, $q \in \Theta \cup \Psi$.

On the other hand, there are some n, such as $n = 3^2 \times 11^2$ or $7^3 \times 19$, such that, if $\Gamma = C_n$, then every Hopf-Galois structure must have type C_n, even though non-abelian groups G of order n exist.

Counting Nilpotent Hopf Galois Structures

A finite group G is **nilpotent** if it is the direct product of its Sylow subgroups,

$$G = \prod_p G_p,$$

(e.g. if G is abelian or a p-group).

Let Γ be nilpotent. Define $e_{\rm nil}(\Gamma)$ to be the number of nilpotent HGS on a Galois extension with group Γ.

This is the number of equivalence classes of regular embeddings

$$\beta : \Gamma \longrightarrow \mathrm{Hol}(G)$$

as G ranges through nilpotent groups of order $|\Gamma|$.

Since each G_p is a *characteristic* subgroup of G (i.e. it is fixed under all automorphisms), we have

$$\mathrm{Aut}(G) = \prod_p \mathrm{Aut}(G_p), \qquad \mathrm{Hol}(G) = \prod_p \mathrm{Hol}(G_p).$$

We are looking for

$$\beta : \prod_p \Gamma_p \longrightarrow \prod_q \mathrm{Hol}(G_q).$$

We can write β as a "matrix" (β_{pq}) where $\beta_{pq} : \Gamma_p \longrightarrow \mathrm{Hol}(G_q)$.

Lemma

β is regular $\Leftrightarrow$ each β_{pp} is regular.

If β is a regular embedding then, for $p \neq q$, the group $\beta_{pq}(\Gamma_p)$ must centralise the regular subgroup $\beta_{qq}(\Gamma_q)$ of $\mathrm{Hol}(G_q)$, so must be a q-group. Hence $\beta_{pq}(\Gamma_p)$ is trivial.

Hence β is a regular embedding if and only if (β_{pq}) is a diagonal matrix whose diagonal entries are regular embeddings.

Hence we have

Theorem

For a nilpotent group Γ*:*

$$e_{\mathrm{nil}}(\Gamma) = \prod_p e_{\mathrm{nil}}(\Gamma_p).$$

Corollary (Nilpotent HGS on cyclic extensions)

Let $r(n) = \prod_{p|n} p$*, the radical of* n*. Then*

$$e_{\mathrm{nil}}(C_n) = \begin{cases} \frac{n}{r(n)} & \text{if } 8 \nmid n; \\ \frac{3}{2}\left(\frac{n}{r(n)}\right) & \text{if } 8 \mid n. \end{cases}$$

(But a cyclic extension may also have HGS which are not nilpotent!)

HGS of nilpotent type

Theorem

Suppose a Galois extension with group Γ admits a HGS of type G, with G nilpotent. Then Γ is soluble.

Recall this means we have subgroups

$$1 = \Gamma_0 \lhd \Gamma_1 \lhd \cdots \lhd \Gamma_s = \Gamma$$

with each Γ_{i+1}/Γ_i abelian.

Let J be a group with $|J| = p^r m$, where p is prime and $p \nmid m$. Then a **Hall p'-subgroup** of J is a subgroup H with $|H| = m$. Unlike Sylow p-subgroups, these don't always exist.

e.g. If $J = A_5$ of order 60, then J has a Hall p'-subgroup for $p = 5$ but not for $p = 2$ or $p = 3$.

In fact, J has a Hall p'-subgroup for every $p \Leftrightarrow J$ is soluble (Hall, 1937).

Now suppose we have a regular embedding

$$\beta : \Gamma \longrightarrow \mathrm{Hol}(G)$$

with $G = \prod_{p} G_p$ nilpotent.

For each p, let

$$H_p = \prod_{q \neq p} G_q,$$

a Hall p'-subgroup of G. Then G_p is characteristic in G. (It consists of all elements of order prime to p.)

Define

$$\Delta_p = \{\gamma \in \Gamma \, | \beta(\gamma) \cdot e_G \in H_p\}.$$

Since $\beta(\Gamma)$ is regular, it is obvious that Δ_p is a *subset* of Γ has size $|H_p|$.

Since H_p is characteristic in G, we can prove:

Lemma

Δ_p is a subgroup *of* Γ*.*

Proof. Let $\gamma \in \Delta_p$, say $\beta(\gamma) \cdot e_G = h \in H_p$.

Then $\beta(\gamma) = (h, \alpha)$ for some $\alpha \in \mathrm{Aut}(G)$.

Given another $\gamma' \in \Delta_p$, say $\beta(\gamma') = (h', \alpha')$, we have

$$\beta(\gamma\gamma') = (h, \alpha)(h', \alpha') = (h\alpha(h'), \alpha\alpha')$$

and $\beta(\gamma\gamma') \cdot e_G = h\alpha(h') \in H_p$ since $\alpha(H_p) = H_p$. So $\gamma\gamma' \in \Delta_p$. □

So Δ_p is a Hall p'-subgroup of Γ.

Since Γ has a Hall p'-subgroup for each p, Γ is soluble.

Must a HGS on an abelian extension be soluble?

Suppose an extension with Galois group Γ admits a HGS of type G.

We have shown that

$$G \text{ nilpotent } \Rightarrow \Gamma \text{ soluble.}$$

Here is a strategy (as yet not completely implemented) to prove a weak converse:

Theorem?

$$\Gamma \textit{ abelian} \Rightarrow G \textit{ soluble},$$

i.e. every HGS on an abelian extension must be soluble.

Remark: One might wonder if Γ soluble $\Leftrightarrow$ G soluble, or, more generally, whether Γ and G always have the same composition factors. This turns out not to be the case. It is not difficult to construct an example with $\Gamma = A_4 \times C_5$ and $G = A_5$. I do not know of any examples where Γ is insoluble but G is soluble.

So suppose Γ is abelian, and we have a regular embedding

$$\beta : \Gamma \hookrightarrow \mathrm{Hol}(G).$$

If H is a characteristic subgroup of G then β induces a homomorphism

$$\overline{\beta} : \Gamma \longrightarrow \mathrm{Hol}(G/H),$$

whose image is a transitive *abelian* subgroup of $\mathrm{Hol}(G/H)$. Hence this image is regular on G/H.

Let $\Sigma = \ker(\overline{\beta})$. Then $|\Sigma| = |H|$ and the abelian group Σ acts regularly on H.

It will suffice to show G/H and H are both soluble.

Inductively, we can therefore reduce to the case where G is *characteristically simple*.

Now a characteristically simple group H has the form

$$H = \underbrace{T \times T \ldots \times T}_{m}$$

for some simple group T and some $m \geq 1$.

So we need to show that we cannot have a regular embedding

$$\Gamma \hookrightarrow \mathrm{Hol}(T^m)$$

where Γ is abelian and T is a **non-abelian** simple group.

In this case

$$\mathrm{Aut}(T^m) = (\mathrm{Aut}(T)^m) \rtimes S_m = \mathrm{Aut}(T) \text{ wr } S_m,$$

where S_m is the symmetric group permuting the m factors.

Aside: Classification of Finite Simple Groups

The finite simple groups are

- cyclic of prime order (the only abelian ones!);
- alternating groups A_n for $n \geq 5$;
- (classical or exceptional) groups of Lie type: there 16 families of these, of which the easiest to describe is

$$\mathrm{PSL}_n(q), \qquad n \geq 2, \quad q \text{ a prime power;}$$

- 26 sporadic simple groups (smallest is the Matthieu group M_{11} of order 7290; largest is the Monster of order approx 8×10^{53}).

Back to HGS on abelian extensions

Can we have a regular embedding of an abelian group Γ in

$$\mathrm{Hol}(T^m) = T^m \rtimes (\mathrm{Aut}(T)^m \rtimes S_m)$$

when T is a non-abelian simple group?

$\mathrm{Aut}(T)$ contains the subgroup of inner automorphisms $\mathrm{Inn}(T) \cong T$, and, as a consequence of the Classification of Finite Simple Groups, we know that the quotient

$$\mathrm{Out}(T) = \frac{\mathrm{Aut}(T)}{\mathrm{Inn}(T)}$$

is (soluble and) small relative to T.

e.g. for T sporadic, $|\mathrm{Out}(T)| \leq 2$.

Projecting Γ into successive quotients in the sequence

$$1 \longrightarrow T^m \longrightarrow (T \rtimes \mathrm{Inn}(T))^m \longrightarrow \mathrm{Hol}(T)^m \longrightarrow \mathrm{Hol}(T)^m \rtimes S_m,$$

we get abelian subgroups

$$\Gamma_1 \leq S_m \qquad \Gamma_2 \leq \mathrm{Out}(T)^m, \qquad \Gamma_3 \leq \mathrm{Inn}(T)^m \cong T^m, \qquad \Gamma_4 \leq T^m$$

such that

$$|\Gamma_1|\,|\Gamma_2|\,|\Gamma_3|\,|\Gamma_4| = |\Gamma| = |T|^m.$$

Why shouldn't this be possible? A non-abelian simple group should not contain a "large" abelian subgroup.

There is a theorem which (almost) guarantees this:

Theorem (Vdovin, 1999)

Let T be a non-abelian simple group not of the form $\mathrm{PSL}_2(q)$, and let A be an abelian subgroup of T. Then $|A|^3 < |T|$.

[Note: $C_5 < A_5$ and $5^3 > 60$. But $A_5 \cong \mathrm{PSL}_2(5) \cong \mathrm{PSL}_2(4)$.]

Proof: Use the Classification of Finite Simple Groups.

It follows that if A is an abelian subgroup of T^m then $|A|^3 < |T^m|$.

Thus, for a particular non-abelian simple group T, if we know $|T|$ and $|\mathrm{Out}(T)|$, we have upper bounds on $|\Gamma_i|$ for $i = 1, \ldots, 4$, and we should be able to show $|\Gamma| < |T^m|$.

This (or a slight variation) works for the alternating groups A_n, for $\mathrm{PSL}_n(q)$ (including $n = 2$) and for the sporadic groups. It still needs to be checked for the other families of groups of Lie type.