Nilpotent algebras and Hopf Galois extensions

Lindsay Childs

Omaha, May 2017

Introduction

The aim of this talk is to describe connections between three apparently different areas of algebra: the theory of Hopf Galois structures, finite permutation group theory and the study of commutative nilpotent $\mathbb{F}_p$-algebras, where p is an odd prime and $\mathbb{F}_p$ is the field of p elements.

We'll begin by determining the ideals of a particular commutative nilpotent $\mathbb{F}_p$-algebra, using nothing but ideas from elementary linear algebra.

Then, beginning with classical Galois theory, we introduce Hopf Galois structures on a Galois extension of fields.

Eventually we will explain how knowledge of the ideals of the example gives information on the image of the Galois correspondence for a Hopf Galois structure on a certain Galois extension of fields whose Galois group is an elementary abelian group of order p^5.

Counting k-dimensional subspaces

We start with some information on the number of subspaces of a finite dimensional $\mathbb{F}_p$-vector space.
Let $s(n, k)$ be the number of k-dimensional subspaces of $A = \mathbb{F}_p^n$. Then

$$s(n, k) = \frac{(p^n - 1)(p^n - p)\cdots(p^n - p^{k-1})}{(p^k - 1)(p^k - p)\cdots(p^k - p^{k-1})}$$

Interpretation: to pick a k-dimensional subspace with a particular basis, pick any non-zero vector v_1 in A ($p^n - 1$ choices), then any vector v_2 not in the space spanned by v_1, etc. That gives the numerator of the formula. Given the space V spanned by $v_1, \ldots, v_k$, we get the same space from any other basis of V, and the number of bases is obtained by picking any vector w_1 in V, then any vector w_2 in V but not in the subspace spanned by v_1, etc. That gives the denominator.

Counting all subspaces

Let $s(n)$ denote the number of subspaces of $\mathbb{F}_p^n$. Then $s(n) = \sum_{k-0}^{n} s(n,k)$. For example, when $n = 5$ we get

$$s(5) = 2p^6 + 2p^5 + 6p^4 + 6p^3 + 6p^2 + 4p + 6.$$

In general, $s(n)$ is a polynomial in p of degree $\lfloor \frac{n^2}{4} \rfloor$. So we have:

n	1	2	3	4	5	6	7	8	9	10
degree of $s(n)$	0	1	2	4	6	9	12	16	20	25

A row space approach to counting

Here is an alternate way to get $s(n)$. We illustrate with $n = 5$. Given A, a five-dimensional vector space with basis $(v_1, v_2, v_3, v_4, v_5)$ over $\mathbb{F}_p$, identify subspaces of A with 5×5 matrices with coefficients in $\mathbb{F}_p$ in reduced row echelon form. Given a basis of A, we can map elements of A to row vectors of coordinates relative to the basis. The subspace of A spanned by elements $a_1, \ldots, a_m$ maps to the row space of the $m \times 5$ matrix whose rows are the coordinates of $a_1, \ldots, a_m$.

Doing row operations to the matrix doesn't change the row space. So the subspaces of A correspond to the set of $m \times 5$ matrices with coefficients in $\mathbb{F}_p$ in reduced row echelon form. Since $\dim(A) = 5$, the echelon matrix of any subspace has at most 5 non-zero rows

Counting row echelon forms

A visual way to count subspaces of A: Just write down all the possible shapes of the echelon forms of 5×5 matrices, and count the number of parameters in each shape. For example, one shape is (124). It looks like

$$\begin{pmatrix} 1 & 0 & \cdot & 0 & \cdot \\ 0 & 1 & \cdot & 0 & \cdot \\ 0 & 0 & 0 & 1 & \cdot \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

There are p^5 possible echelon matrices of this shape, because there are five free parameters (the entries denoted by $\cdot$). The shape (12345) has no free parameters. The shapes (12) and (123) have six free parameters. That helps explain why $s(5)$ is a polynomial in p of degree 6.

There are $2^5 = 32$ shapes. (For large n this method is not practical!)

A commutative nilpotent $\mathbb{F}_p$-algebra

Let A be the free commutative $\mathbb{F}_p$-algebra (without unit) generated by elements x and y, modulo the relations $A^3 = 0$. Thus A has a basis as a vector space over $\mathbb{F}_p$ consisting of x, y, x^2, xy, y^2, and
$x^3 = x^2y = xy^2 = y^3 = 0$. As a vector space, $A \cong \mathbb{F}_p^5$.
An ideal of A is a subspace of A closed under multiplication by elements of A. For example, the ideal generated by x, denoted $G(x)$, is the subspace $\mathbb{F}_p x + Ax$ and has an $\mathbb{F}_p$-basis (x, x^2, xy). The ideal $G(x, y) = A$.

Ideals of A

Let $i(A)$ denote the number of ideals of A. I want to compute $i(A)$. Any ideal of A that contains

$$u = ax + by + cx^2 + dxy + ey^2$$

also contains $xu = ax^2 + bxy$ and $yu = axy + by^2$.
So we can take the echelon forms of subspaces, and see what the echelon forms are when we adjoin rows that correspond to taking the elements u corresponding to existing rows and multiply them by x and y.
For example, it's easy to see that the subspaces of A whose echelon forms are among the eight shapes $(12\ldots)$ are exactly the subspaces that generate the ideal A.

For a slightly more complicated example, an echelon form (14) looks like

$$\begin{pmatrix} 1 & b & c & 0 & e \\ 0 & 0 & 0 & 1 & f \end{pmatrix}.$$

If $b = f$ then the subspace generates the ideal

$$J_1(b, e') = G(x + by + e'y^2)$$

for $e' = e + b^2c$. If $b \neq f$ then it generates the ideal

$$J_{15}(b) = G(x + by, y^2).$$

The ideals of A

Looking at all of the echelon forms, it's not hard to see that A has the following ideals: the subscripts denote the shape of the echelon form of the subspace spanned by the generators of the ideal.

$$\begin{aligned} A &= \langle x, y\rangle \\ J_1(a, d) &= \langle x + ay + dy^2\rangle \\ J_{1,5}(a) &= \langle x + ay, y^2\rangle \\ J_2(b) &= \langle y + bx^2\rangle \\ J_{2,3} &= \langle y, x^2\rangle \end{aligned}$$

subspaces of (x^2, xy, y^2).

So we can count the ideals of A by counting the number of parameters in ideals of each type:

$$\begin{aligned} 1 + p^2 + p + p + 1 + s(3) &= p^2 + 2p + 2 + (2p^2 + 2p + 4) \\ &= 3p^2 + 4p + 6. \end{aligned}$$

Poonen's list

The algebra $A = \langle x, y \rangle$ is one of the 25 isomorphism types of commutative local algebras of dimension 5 classified in a paper, " Isomorphism types of commutative algebras of finite rank over an algebraically closed field" by Bjorn Poonen (2007).

Why am I interested in this?

It connects with Galois theory.

Galois (1832)

Given a polynomial

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

with coefficients in a field K, let L be the smallest field containing K and all roots of $f(x)$. Galois introduced the finite group G of all of those permutations of the roots of $f(x)$ that respect the algebraic relationships (over K) of the roots.
The group G is called the Galois group of L/K. Call L/K a Galois extension with Galois group G.

The Galois correspondence

For L/K a Galois extension with Galois group G, there is a map from the subgroups H of G to the fields N with $K \subseteq N \subseteq L$, given by $H \to L^H =$ the set of all elements of L that are fixed by the permutations in H.
The Fundamental Theorem of Galois Theory (FTGT) says: this map is bijective. (Corollary: for $K = \mathbb{Q}$, L/K a Galois extension with Galois group G, there is only a finite number of subgroups of G, hence only finitely many subfields of L containing K. By contrast, there are infinitely many K-subspaces of L.)

Evolution of Galois theory

It took close to two generations for mathematicians to understand Galois, long after his death in a duel at age 20 in 1832. First exposition in books: Serret (1866), Jordan (1870). With the development of linear algebra, then module theory, the theory was reformulated, especially by Emil Artin in 1942, into a framework that suggested generalization. An early example was by N. Jacobson, 1937, 1944, who developed a Galois theory for purely inseparable field extensions of exponent 1. One objective was to try to get a FTGT.

CHR

In 1965, Chase, Harrison and Rosenberg developed a generalization of Galois theory for extensions S/R of commutative rings and G a group of R-algebra automorphisms of S. The characteristic properties defining S/R with group G as a Galois extension of commutative rings are

(i) $S \otimes_R S \cong \mathrm{Hom}(G, S)$ $(= S \times S \times \ldots \times S)$ by

$$s \otimes t \mapsto h(s \otimes t) \text{ where } h(s \otimes t)(g) = sg(t).$$

(Note: if $S = R[x]/(p(x))$ and $p(x)$ splits in S, then

$$S[x]/(p(x)) \cong S \times ... \times S)$$

(ii) The map $j : S[G] \to \mathrm{End}_R(S)$ by $j(sg)(t) = sg(t)$ is bijective. (“linear independence of characters")

These are equivalent conditions.

If S has no idempotents other than 0 and 1, then the FTGT (in particular, surjectivity of the Galois correspondence) holds for these Galois extensions.

CHR for valuation rings

If S, R are valuation rings of local fields L/K and L/K is a classical Galois extension with Galois group G, then S/R is a Galois extension with Galois group G if and only if L/K is unramified.

Hopf Galois extensions

In 1968, Chase and Sweedler developed a Hopf algebra version of Galois theory, building on the above ideas.
If L/K is a Galois extension of fields with Galois group G, then L becomes a KG-module, where an element $(\sum_i s_i g_i)$ acts on t in L by $(\sum s_i g_i)(t) = \sum_i s_i g_i(t)$.
The idea is to replace the group ring KG by a K-Hopf algebra H that acts on L as an H-module algebra.

K-Hopf algebra

A K-Hopf algebra H is a K-algebra (addition, multiplication, scalar multiplication by elements of K) with three more maps:
A comultiplication $\Delta : H \to H \otimes_K H$.
A counit $\epsilon : H \to K$.
These satisfy properties such that if you take the dual $H^* = \mathrm{Hom}_K(H, K)$ and the dual maps $\Delta* : H^* \otimes_K H^* \to H^*$, $\epsilon* : K \to H^*$, then H^* is a K-algebra.
Also Δ and ϵ should be K-algebra homomorphisms.
Also, a Hopf algebra has an antipode or coinverse map: $s : H \to H$. s is a K-algebra antihomomorphism: $s(hk) = s(k)s(h)$.
Example: KG with $\Delta(g) = g \otimes g$, $\epsilon(g) = 1$, $s(g) = g^{-1}$.
If H^* is a commutative K-algebra then H is called cocommutative. KG is cocommutative for all finite groups G.

Hopf Galois structures

(Chase and Sweedler) Let L/K be a field extension, H a cocommutative K-Hopf algebra so that L is an H-module algebra. Then L/K is an H-Hopf Galois extension if the map $j : L \otimes_K H \to \mathrm{End}_K(L)$ given by $j(s \otimes h)(t) = sh(t)$ is a bijection.

The classical case: if L/K is a Galois extension with Galois group Γ, then L/K is a $K\Gamma$-Hopf Galois extension.

Chase and Sweedler developed the Galois correspondence from subHopf algebras of H to subfields of L containing K.
BUT: in contrast to the case of commutative rings with no non-trivial idempotents, they couldn't prove surjectivity–no FTGT.

Greither-Pareigis

In 1987 Greither and Paregis looked at Chase and Sweedler's theory in the case where it seemed not to be needed: Galois extensions of fields. They found that a classical Galois extension of fields L/K with Galois group Γ might also be a Hopf Galois extension for a K-Hopf algebra other than $H = K\Gamma$. And they transformed the problem of finding Hopf Galois structures on L/K into a problem in finite permutation group theory.

Greither-Pareigis, ctd.

Suppose L/K is a Galois extension with Galois group Γ.
Then from the definition of Hopf Galois extension,

$$L \otimes_K L \cong \Gamma L = \oplus_{\gamma \in \Gamma} L e_\gamma$$

where $\{e_\gamma : \gamma \in \Gamma\}$ is a dual basis to the elements γ of Γ.
If L/K is also an H-Galois extension, then taking the module action

$$H \otimes_K L \to L$$

and tensoring over K with L ("base change to L") yields an action

$$(L \otimes_K H) \otimes_K (L \otimes_K L) \to (L \otimes_K L)$$

or

$$(L \otimes_K H) \otimes_K \Gamma L \to \Gamma L$$

making ΓL an $L \otimes_K H$ -Galois extension.

The key idea of [GP87]

Looking at the isomorphism

$$(L \otimes_K H) \otimes_K \Gamma L \to \Gamma L,$$

[GP87] observed that $L \otimes_K H$ must = LN where N acts on ΓL as a regular group of permutations of the dual basis of Γ, and is normalized in *Perm*(Γ) by the image $\lambda(\Gamma)$ of the left regular representation $\lambda : \Gamma \to \mathrm{Perm}(\Gamma)$ by $\lambda(g)(h) = gh$.
The group N is called the *type* of H or of the Hopf Galois extension L/K.

A problem in finite permutation group theory

Greither-Pareigis's base change result is reversible: let N be a regular subgroup of $Perm(\Gamma)$ that is normalized by $\lambda(\Gamma)$: for all n in N, $\lambda(g)$ in $\lambda(\Gamma)$,

$$\lambda(g)n\lambda(g)^{-1} = n'$$

for some n' in N. Then there is a K-Hopf algebra $H = (LN)^{\Gamma}$, that acts on L and makes L/K into an H-Hopf Galois extension.

Summing up [GP87]

To find the Hopf Galois structures on L/K with Galois group Γ, find the regular subgroups N of $\mathrm{Perm}(\Gamma)$ that are normalized by $\lambda(\Gamma)$. But: $\mathrm{Perm}(\Gamma)$ is huge. Few results (except for Tim Kohl) with this direct approach, except for one nice result of Greither-Pareigis.

[GP87] and FTGT

One subgroup of $\mathrm{Perm}(\Gamma)$ normalized by $\lambda(\Gamma)$ is $\rho(\Gamma)$, the image of the right regular representation $(\rho(\gamma)(\delta) = \gamma\delta^{-1}$. In fact, $\lambda(\Gamma)$ centralizes $\rho(\Gamma)$. So $\rho(\Gamma)$ corresponds to the K-Hopf algebra KG – it is the subgroup of $\mathrm{Perm}(\Gamma)$ corresponding to the classical Hopf Galois structure given by the Galois group Γ.

But for G non-abelian, another subgroup of $\mathrm{Perm}(\Gamma)$ normalized by $\lambda(\Gamma)$ is $\lambda(\Gamma)$ itself. It turns out that the corresponding K-Hopf algebra H_λ is not the group ring $K\Gamma$, and under the Galois correspondence of Chase and Sweedler, the intermediate fields F that come from sub-Hopf algebras of H_λ are the fields F so that F/K is normal. So unless every subgroup of Γ is normal, the Galois correspondence of Chase and Sweedler is not surjective.
FTGT fails for Hopf Galois extensions.

Byott reformulated the Greither-Pareigis problem.

Given a regular subgroup N of $\mathrm{Perm}(\Gamma)$ normalized by $\lambda(\Gamma)$, let G be an abstract group with $\#G = \#\Gamma$, and suppose $\alpha : G \to \mathrm{Perm}(\Gamma)$ is a 1-1 group homomorphism with image N. Let $a : G \to \Gamma$ be defined by $a(g) = \alpha(g)(e_\Gamma)$. Then a is a bijection (by the regularity of N). Then α can be recovered by

$$\alpha(g)(\gamma) = a(\lambda_G(g)(a^{-1}(\gamma))),$$

and we may define a unique 1-1 group homomorphism $\beta : \Gamma \to \mathrm{Perm}(G)$ by

$$\beta(\gamma)(g) = a^{-1}(\lambda_\Gamma(\gamma)(a(g))),$$

whose image $T = \beta(\Gamma)$ is a regular subgroup of $\mathrm{Perm}(G)$, and T normalizes $\lambda(G)$ inside $\mathrm{Perm}(G)$.

The normalizer of $\lambda(G)$ inside $\mathrm{Perm}(G)$ is a well-known subgroup of $\mathrm{Perm}(G)$, called the holomorph $\mathrm{Hol}(G)$ of G. It is isomorphic to the semidirect product of G and $\mathrm{Aut}(G)$.

Conversely...

Conversely, given T, a regular subgroup isomorphic to Γ in $\mathrm{Hol}(G)$ for $|G| = |\Gamma|$, let $\beta : \Gamma \to \mathrm{Hol}(G)$ be an isomorphism onto T. Then reversing the above construction yields $\alpha : G \to \mathrm{Perm}(\Gamma)$ whose image is a regular subgroup of $\mathrm{Perm}(\Gamma)$ normalized by $\lambda(\Gamma)$, hence yields a Hopf Galois structure on L/K of type G.

Thus, given L/K with Galois group Γ, to find Hopf Galois structures on L/K of type G, we can look for regular subgroups T of $\mathrm{Hol}(G)$ that are isomorphic to Γ.

This is an easier problem: $\mathrm{Hol}(G)$ is far smaller than $\mathrm{Perm}(\Gamma)$.

Working with the holomorph has yielded some very nice results. For example:

Byott's uniqueness result

By studying regular subgroups of holomorphs, Byott (1996) was able to characterize those Galois extensions L/K with Galois group Γ that have no Hopf Galois structures other than the classical one. The condition: the order n of G should be coprime to $\phi(n)$. (That implies that G is cyclic of square-free order.)

Γ a non-abelian simple group

For L/K Galois with non-abelian simple group Γ, Carnahan and Childs (1999) looked at regular embeddings of Γ into $\mathrm{Hol}(\Gamma) = \Gamma \cdot Aut(\Gamma)$. Using that $Aut(\Gamma)/Inn(\Gamma)$ is solvable, and Γ has no fixed-point free automorphisms (two consequences of the classification of finite simple groups), we showed that any regular embedding had to map into $\Gamma \cdot Inn(\Gamma)$ and then that there are only two possibilities for Hopf Galois structures of type Γ, namely the ones corresponding to the two Hopf Galois structures of Greither and Pareigis.

Byott (2004) subsequently showed that there were no Hopf Galois structures of type G for any G other than Γ, by showing that for A a non-abelian simple group there is no group B not isomorphic to A for which there is a regular embedding of A into $Hol(B)$.

Two recent results using the holomorph

Byott and Childs (2012) proved that if Γ is a non-cyclic abelian p-group of order p^n, $n \geq 3$, then L/K has a Hopf Galois structure of non-abelian type.

Byott (2015) proved that if Γ is an abelian group, and L/K has a Hopf Galois structure of type G, then G must be solvable.

Specialize to $\Gamma = (\mathbb{F}_p^n, +)$

Now specialize to the case where $\Gamma = (\mathbb{F}_p^n, +)$ is an elementary abelian p-group. Problem: find regular subgroups $T \cong \Gamma$ of $\mathrm{Hol}(G)$ where $G \cong \Gamma$ is also an elementary abelian p-group.

In that case there is a bijection:

Regular subgroups of $\mathrm{Hol}(\Gamma)$ isomorphic to Γ

$$\updownarrow$$

$\{$Nilpotent (associative, commutative) algebra structures A on $(\Gamma, +)$ with $A^p = 0\}$.

How it works

This correspondence comes from Caranti, et. al. (2006).
Let $(G,+)$ be a finite abelian p-group. Let $A=(G,+,\cdot)$ be a commutative, associative nilpotent $\mathbb{F}_p$-algebra (hereafter, "nilpotent") so that $(A,+)=(G,+)$. Define the circle operation on A by

$$g\circ h=g+h+g\cdot h.$$

Then $(G,\circ)$ is a finite abelian p-group. Define $\tau:(G,\circ)\to\mathrm{Perm}(G,+)$ by $\tau(g)(x)=g\circ x$. Then $T=\tau(G,\circ)$ is a regular subgroup of $\mathrm{Hol}(G)$. Conversely, given a regular abelian subgroup T of $\mathrm{Hol}(G,+)$, there is a nilpotent ring structure $A=(G,+,\cdot)$ on G, which defines the $\circ$ operation as above and yields a unique isomorphism $\tau:(G,\circ)\to T$ so that $\tau(g)(x)=g\circ x$.

Our example

Returning to our example at the beginning, let $G = (\mathbb{F}_p^5, +)$ and identify G as the additive group of $A = \langle x, y \rangle$ with $A^3 = 0$. Then $(A, \circ) = T$ acts on $(A, +) = G$ by

$$\begin{aligned} \tau(x^2)(u) &= x^2 + u \\ \tau(xy)(u) &= xy + u \\ \tau(y^2)(u) &= y^2 + u \\ \tau(x)(u) &= x + u + xu \\ \tau(y)(u) &= y + u + yu. \end{aligned}$$

Uses of nilpotent algebra structures

For $G = (\mathbb{F}_p^n, +)$ an elementary abelian p-group, the correspondence between regular subgroups of $\mathrm{Hol}(G)$ of type Γ where $\Gamma \cong G$, and commutative nilpotent algebra structures A on $(G, +)$ with $A^p = 0$ has turned out to be useful in several ways.

To count Hopf Galois structures

Using ideas that go back to the 1970's (Kruse and Price) along with more recent results of B. Poonen, one finds that the number of Hopf Galois structures of type G on a Galois extension L/K with Galois group G is asymptotic to

$$p^{(\frac{2}{27})n^3}$$

as $n \to \infty$.

For $n \geq 6$ the number of Hopf Galois structures of type $(\mathbb{F}_p^n, +)$ goes to infinity with p. The case $n = 5$ remains open.

To study the Galois correspondence

Here is an application of nilpotent algebras to the image of the Galois correspondence for Hopf Galois extensions on Galois extensions with Galois group $\Gamma = (\mathbb{F}_p^n, +)$

Theorem

Let G be a finite abelian p-group, written additively. Let $A = (G, +, \cdot)$be a commutative nilpotent algebra structure on $(G, +)$ that yields a regular embedding $\alpha : (G, +) \to \mathrm{Perm}(\Gamma)$ whose image is normalized by $\lambda(\Gamma)$. Let L/K be a Galois extension of fields with Galois group Γ and is a H-Hopf Galois extension corresponding to $\alpha(G, +)$. Then the lattice (under inclusion) of K-sub-Hopf algebras of H, is isomorphic to the lattice of ideals of A.

On the image of the Galois correspondence

Example. Let $p \geq 3$, let L/K be a Galois extension with Galois group $\Gamma = (\mathbb{F}_p^5, +)$, and suppose L/K is a H-Hopf Galois extension, where the Hopf Galois extension corresponds to the regular subgroup $T = \tau(A)$ of $\mathrm{Hol}(\Gamma)$ coming from our example $A = \langle x, y \rangle$ with $A^3 = 0$. Then there are

$$s(A) = s(5) = 2p^6 + 2p^5 + 6p^4 + 6p^3 + 6p^2 + 4p + 6$$

intermediate fields, but only

$$i(A) = 3p^2 + 4p + 6$$

K-subHopf algebras of H, and hence only $i(A)$ intermediate fields in the image of the Galois correspondence for that Hopf Galois structure on L/K.
For this Hopf Galois structure we have quantified precisely how far the Galois correspondence is from being surjective.

Failure of the FTGT

In general, the connection between Hopf Galois structures of type Γ on Galois extensions L/K with Galois group Γ, an elementary abelian p-group and nilpotent algebra structures on $(\Gamma, +)$ yields the result that an H-Hopf Galois structure on L/K satisfies the FTGT (that is, the Galois correspondence is surjective) if and only if H is the classical Galois structure by $K\Gamma$ on L/K.

Summary

What I tried to demonstrate in this talk is an interconnectedness among three areas of algebra: generalizations of classical Galois theory of fields, finite permutation group theory, and finite commutative nilpotent algebras. Finding those connections makes studying each of the areas much richer, because ideas, results and techniques from one area can be applied to another area. For example, Byott's (2015) result that a classical Galois extension with abelian Galois group cannot have a Hopf Galois structure of non-solvable type turned out to be a consequence of a result of C. H. Li (2003), a group theorist, in a paper that solved a century-old problem of Burnside on finite permutation groups.

Summary

You'll see more interconnectivity this week. The connection Caranti, della Volta and Sala made between abelian regular subgroups of the holomorph of an abelian group and finite commutative nilpotent algebras has been generalized to a connection between left braces and regular subgroups of the holomorph of a not-necessarily abelian finite group. A left and right brace is a commutative nilpotent algebra. Left braces yield solutions of the Yang-Baxter equation, of interest in statistical mechanics and elsewhere. So since the invention of braces ten years ago there have been many papers about them.

Brace results

Brace theorists have recently discovered the Hopf Galois theory literature:
A paper, “Solutions of the Yang-Baxter equation associated to skew left braces, with applications to racks," by David Bachiller (Arxiv, 24 Nov. 2016) states:
“To find regular subgroups of $\mathrm{Hol}(G)$ is equivalent to find skew left braces with star group isomorphic to G”.
So:
“Skew left braces of order pq are completely classified” (Byott, 2004)
“Skew left braces with multiplicative group equal to a finite simple group are completely classified” (Carnahan and Childs, 1999), (Byott, 2004)
Also cited is (Byott, 2015) where he showed that an abelian Galois extension of fields cannot have a Hopf Galois structure of non-solvable type.

I guess we Hopf Galois theorists need to study brace theory. Nigel will be talking about braces on Wednesday.

If anyone wants to compute the ratio $i(A)/s(A)$ for some commutative nilpotent algebras, I have copies of Poonen's list available.

Thank you.