Commutative nilpotent rings and Hopf Galois structures

Lindsay Childs

Exeter, June, 2015

Hopf Galois structures

Let L/K be a field extension, H a cocommutative K-Hopf algebra. Then L/K is an H-Hopf Galois extension if L is an H-module algebra and the map $j : L \otimes_K H \to End_K(L)$ induced from the H-module structure on L is a bijection.
If L/K is a Galois extension with Galois group G, then L/K is a KG-Hopf Galois extension.
Assume that L/K is a Galois extension of fields with Galois group Γ. Greither and Pareigis [GP87] showed that Hopf Galois structures on L/K are in bijective correspondence with regular subgroups of $\mathrm{Perm}(\Gamma)$ that are normalized by $\lambda(\Gamma) =$ the image in $\mathrm{Perm}(\Gamma)$ of the left regular representation $\lambda : \Gamma \to \mathrm{Perm}(\Gamma), \lambda(g)(x) = gx$ for g, x in Γ. So the number of Hopf Galois structures on L/K depends only on the Galois group $\Gamma = Gal(L/K)$.

The type of T

If T is a regular subgroup of $\mathrm{Perm}(\Gamma)$ normalized by $\lambda(\Gamma)$, then the corresponding Hopf Galois structure on L/K is said to have type G if $T \cong G$.

A sample of results

• [GP87] A Galois extension with non-abelian Galois group has at least two Hopf Galois structures.
• [By96] A Galois extension with Galois group of order n has a unique Hopf Galois structure if and only if $(n, \phi(n)) = 1$.
• [Ch03] There exist non-abelian groups Γ so that a Galois extension with Galois group Γ has Hopf Galois structures of type G for every isomorphism type of group G of the same cardinality as Γ.
• [CC99] if $\Gamma = S_n$ for $n \geq 5$ then there are at least $\sqrt{n!}$ Hopf Galois structures on L/K.
• [BC12] If Γ is a non-cyclic abelian p-group of order p^n, $n \geq 3$, or is an abelian group of even order $n > 4$, then L/K admits a non-abelian Hopf Galois structure.
• [By04] if Γ is a non-abelian simple group, then L/K has exactly two Hopf Galois structures.

Motivation

Let L/K be a Galois extension of local fields of residue characteristic p and Galois group Γ. Local Galois module theory attempts to understand the structure of the valuation ring $\mathfrak{O}_L$ as a module over $\mathfrak{O}_K\Gamma$, or, if L/K is totally ramified case, over $\mathfrak{A}$, the associated order of $\mathfrak{O}_L$ in $\mathfrak{O}_K\Gamma$.

If L/K is H-Galois, then one can look at $\mathfrak{O}_L$ as a module over the associated order $\mathfrak{A}_H$ in H. If $\mathfrak{A}$ is a Hopf order, then $\mathfrak{O}_L$ is free over $\mathfrak{A}$. [By00] has many examples of Kummer extensions for an isogeny of Lubin-Tate formal groups, where $\mathfrak{O}_L$ is not free over its associated order in $K\Gamma$ but is free over its associated order in the Hopf algebra H arising from the isogeny of the formal group.

In [By02] Byott studied the case of Galois extensions L/K of local fields with cyclic or elementary abelian Galois group Γ of order p^2. For G elementary abelian and p odd, there are L/K with a unique Hopf Galois structure, non-classical, for which the associated order $\mathfrak{A}$ is a Hopf order and $\mathfrak{O}_L$ is free over $\mathfrak{A}$.

This talk

This talk deals entirely with Hopf Galois structures on Galois extensions L/K with Galois group an elementary abelian p-group of order p^n, p odd. This case has drawn a significant amount of interest in local Galois module theory, for example involving applications of scaffold theory and constructions of Hopf orders by several participants in the conference.
The first part of the talk is a summary of results from [Ch15] on the number of Hopf Galois structures on a Galois extension L/K with Galois group $G = C_p^n$ for n large. The second part is more recent work.

Translation to the holomorph

Let L/K be Galois with group Γ. A standard method to find, or at least to count Hopf Galois structures on L/K of type G, is to transform the problem to the holomorph $\mathrm{Hol}(G), =$ the normalizer of $\lambda(G)$ in $\mathrm{Perm}(G)$, where $\lambda : G \to \mathrm{Perm}(G)$ is the left regular representation.

$$\mathrm{Hol}(G) = \rho(G) \cdot Aut(G) \subset \mathrm{Perm}(G)$$

where $\rho(G)$ is the image of the right regular representation. As first explicitly shown in [By96], there is a bijection between Hopf Galois structures of type G and equivalence classes of regular embeddings $\beta : \Gamma \to \mathrm{Hol}(G)$, where $\beta \sim \beta'$ if there is an automorphism θ of G so that

$$\theta\beta(\gamma)\theta^{-1} = \beta'(\gamma)$$

for all γ in Γ.
Transformation to the holomorph has yielded most of the known results on the cardinality of Hopf Galois structures, and in particular, most of the results cited above (but not those in [By02]).

Counting Hopf Galois structures for $G \cong (\mathbb{F}_p^n, +)$

Let $\Gamma \cong G$ be elementary abelian of order p^n. To count the number of Hopf Galois structures of type G, we count regular subgroups of

$$\begin{aligned} \mathrm{Hol}(G) &\cong \mathrm{Aff}_n(\mathbb{F}_p) \\ &= \begin{pmatrix} \mathrm{GL}_n(\mathbb{F}_p) & \mathbb{F}_p^n \\ 0 & 1 \end{pmatrix} \\ &\subset \mathrm{GL}_{n+1}(\mathbb{F}_p). \end{aligned}$$

A nice tool: use a result of [CDVS06] to transform the problem into one of finding isomorphism types of commutative nilpotent $\mathbb{F}_p$-algebra structures on $(\mathbb{F}_p, +)$.

Algebras to regular subgroups...

Let $(G, +)$ be a finite elementary abelian p-group. Let A be a commutative nilpotent algebra structure $(G, +, \cdot)$ on G. Define a group operation $\circ$ on the set G by

$$x \circ y = x + y + x \cdot y.$$

Then $N = (G, \circ)$ is a group (because A is nilpotent), the group associated to A. Define an embedding

$$\tau : N \to \mathrm{Hol}(G) \subset \mathrm{Perm}(G)$$

by

$$\tau(x)(z) = x \circ z = x + z + x \cdot z$$

for all z in G. Then $T = \tau(N)$ is a regular subgroup of $\mathrm{Hol}(G)$ because $\tau(x)(0) = x \circ 0 = x$ for all x in G.

...and back

Conversely, if T is an abelian regular subgroup of $\mathrm{Hol}(G)$, then

$$T = \{\tau(x) \in \mathrm{Hol}(G) : x \in G\}$$

where $\tau(x)(0) = x$ for all x. Use the multiplication in $\mathrm{Hol}(G)$ to define a new group structure on G by $\tau(x)\tau(y) = \tau(x \circ y)$. Then define a multiplication on $(G, +)$ by $x \cdot y = x \circ y - x - y$. This multiplication makes $(G, +, \cdot)$ into a commutative nilpotent $\mathbb{F}_p$-algebra.

[CDVS06] prove that two commutative nilpotent $\mathbb{F}_p$-algebras are isomorphic iff the corresponding regular subgroups of $\mathrm{Aff}_n(\mathbb{F}_p)$ are in the same orbit under conjugation by elements of $\mathrm{Aut}(G) = \mathrm{GL}_n(\mathbb{F}_p)$.

Isomorphism types of algebras

Determining the isomorphism types of commutative nilpotent $\mathbb{F}_p$-algebras of dimension n is a non-trivial problem (c.f. [Po08b]). But an estimate of their number is possible.

There are several reasons why it is useful to focus on commutative nilpotent $\mathbb{F}_p$-algebras A with $A^3 = 0$.

Reason # 1: A lower bound on algebras A with $A^3 = 0$

Let $f_3(n, r) =$ the number of isomorphism types of commutative $\mathbb{F}_p$-algebras N with $\dim_{\mathbb{F}_p} A = n, \dim_{\mathbb{F}_p}(A/A^2) = r$, and $A^3 = 0$. Then

$$f_3(n, r) \geq p^{(\frac{r^2+r}{2})(n-r)-(n-r)^2-r^2}.$$

The idea is from Kruse and Price [KP70] ...

Multiplications on G

Let A have $A^3 = 0$. Let $\mu : A \times A \to A$ be the multiplication. Then μ is uniquely determined by a map

$$\overline{\mu} : A/A^2 \times A/A^2 \to A^2,$$

Let A have an $\mathbb{F}_p$-basis $\{x_1, \ldots, x_r, y_1, \ldots, y_{n-r}\}$ where the first r elements define modulo A^2 a basis $(\overline{x}_1, \ldots, \overline{x}_r)$ of A/A^2 and $(y_1, \ldots, y_{n-r})$ is a basis of A^2. The ring structure on A is then defined by $n - r$ structure matrices $\Phi^{(k)} = (\phi_{i,j}^{(k)})$ defined by

$$\overline{x}_i \overline{x}_j = \sum_{k=1}^{n-r} \phi_{i,j}^{(k)} y_k.$$

Conversely, any set of $n - r$ symmetric matrices $\Phi^{(k)}$ defines a map $\mu : A \times A \to A$ which is commutative, and associative because $A^3 = 0$. So each choice of the symmetric structure matrices

$$\{\Phi^{(k)} | k = 1, \ldots, n - r\}$$

defines a commutative nilpotent algebra structure.

Isomorphism types

Let $\mathcal{S} = \{\{\Phi^{(1)}, \ldots, \Phi^{(n-r)}\}\}$ be the set of all possible sets of $r \times r$ symmetric matrices. Then

$$|\mathcal{S}| = p^{(n-r)(\frac{r^2+r}{2})}.$$

The group $H = \mathrm{GL}_{n-r}(\mathbb{F}_p) \times \mathrm{GL}_r(\mathbb{F}_p)$ acts on the set of bases for A/A^2 and A^2, hence on the set $\mathcal{S}$ of sets of symmetric matrices .
Two sets of symmetric matrices in the same orbit under the action of H define isomorphic $\mathbb{F}_p$-algebras, and conversely. So

$$f_3(n, r) = \#\text{ of orbits in } \mathcal{S} \text{ under the action of } H.$$

So

$$|\mathcal{S}| = \sum_{orbits} \#\text{ of elements in each orbit}$$
$$\leq \sum_{orbits} |H| = f_3(n, r) \cdot |H|.$$

Bounding $f_3(n, r)$

Hence

$$f_3(n,r) \geq \frac{|\mathcal{S}|}{|H|} = \frac{p^{(\frac{r^2+r}{2})(n-r)}}{|\mathrm{GL}_{n-r}(\mathbb{F}_p)| \cdot |\mathrm{GL}_r(\mathbb{F}_p)|}.$$

Now $|\mathrm{GL}_k(\mathbb{F}_p) < p^{k^2}$, so

$$f_3(n,r) \geq \frac{p^{(\frac{r^2+r}{2})(n-r)}}{p^{(n-r)^2+r^2}} = p^b$$

where

$$b = (\frac{r^2+r}{2})(n-r) - ((n-r)^2 + r^2).$$

Done.

A bound on isomorphism types of algebras A with $A^3 = 0$

Setting $f_3(n) = \sum_r f_3(n, r)$ and setting $r = 2n/3$ gives

$$f_3(n) \geq f_3(n, 2n/3) \geq p^{\frac{2n^3}{27} - \frac{4n^2}{9}}.$$

Reason # 2 : Approximating the number of Hopf Galois structures of type G

The number of Hopf Galois structures of type G on a Galois extension L/K with Galois group G is equal to the number $|R(G,[G])|$ of regular subgroups of $\mathrm{Perm}(G)$ isomorphic to G that are normalized by $\lambda(G)$.
By a formula in [By96],

$$|R(G,[G])| = |S(G,[G])|$$

where $S(G,[G])$ is the number of regular subgroups $N \cong G$ of $\mathrm{Hol}(G)$.

A regular subgroup N arising from a comm. nilpotent algebra A is isomorphic to G iff $A^p = 0$ (c.f. [FCC12]) .
Let $f_p(n) = \#$ of isomorphism types of A with $A^p = 0$.

An upper bound

For each isomorphism type A of commutative nilpotent algebra the number of regular subgroups of $\mathrm{Hol}(G)$ corresponding to A is equal to the size of the orbit under $\mathrm{GL}_n(\mathbb{F}_p) = \mathrm{Aut}(G)$ of one regular subgroup corresponding to A. So

$$f_p(n) \leq |S(G, [G])| \leq f_p(n) \cdot |\mathrm{GL}_n(\mathbb{F}_p)|.$$

Of course $|\mathrm{GL}_n(\mathbb{F}_p)| \leq p^{n^2}$.
A result of Poonen [Po08a] yields

$$f_p(n) \leq p^{\frac{2}{27}n^3 + O(n^{8/3})},$$

so

$$|R(G, [G])| = |S(G, [G])| \leq p^{\frac{2}{27}n^3 + O(n^{8/3})} \cdot p^{n^2},$$

so

The point

Let G be an elementary abelian p-group of order p^n, L/K a Galois extension of fields with Galois group G. Then the number $|R(G,[G])|$ of Hopf Galois structures of type G on L/K satisfies

$$p^{\frac{2}{27}n^3-\frac{4}{9}n^2} \leq f_3(n) \leq |R(G,[G])| \leq p^{\frac{2}{27}n^3+O(n^{8/3})}.$$

For large n, the number of Hopf Galois structures of type G on L/K arising from algebras A with $A^3 = 0$ is of the same order of magnitude as the set of all Hopf Galois structures of type G.

Reason # 3: Algebras A with $A^3 = 0$ yield Hopf Galois structures directly by descent

The rest of this talk is post [Ch15].
As always, $G \cong (\mathbb{F}_p^n, +)$.
Given a commutative nilpotent algebra A and a fixed basis of A, we obtain a regular subgroup T of $\mathrm{Hol}(G)$. If $A^p = 0$, then the regular subgroup is isomorphic to G. To find Hopf Galois structures on a Galois extension L/K with Galois group $\Gamma \cong G$ from such algebras, the usual way is to translate from the holomorph to $\mathrm{Perm}(G)$:

comm. algs A, $A^p = 0$
with fixed basis

$\downarrow$

reg. subgps $T \cong G$
of $\mathrm{Hol}(G)$

$\downarrow$

equiv. classes of
$\beta : G \to T \subset \mathrm{Hol}(G)$ $\longleftrightarrow$ $M \cong G \subset \mathrm{Perm}(G)$
normalized by $\lambda(G)$

$\updownarrow$

Hopf Galois structures of type G

When $A^3 = 0$

But if $A^3 = 0$, we can proceed more directly.
Proposition: Given a commutative nilpotent $\mathbb{F}_p$-algebra A and an associated regular subgroup $T \subset \mathrm{Perm}(G)$, then T is normalized by $\lambda(G)$, the image in $\mathrm{Perm}(G)$ of the left regular representation of G, if and only if $A^3 = 0$.

So if $A^3 = 0$, the picture becomes

comm. algs A with $A^3 = 0$

$\downarrow$

regular subgroups $T \cong G$
of $\mathrm{Hol}(G) \subset \mathrm{Perm}(G)$ normalized by $\lambda(G)$

$\updownarrow$

Hopf Galois structures of type G

Sketch of proof

Suppose A is a comm. nilpotent algebra, $T = \{\tau(x) : x \in A\} \subset \mathrm{Hol}(G)$. We have that for all z in G,

$$\tau(x)(z) = x + z + x \cdot z$$

while

$$\lambda(y)(z) = y + z.$$

Then T is normalized by $\lambda(G)$ iff for all x, y in A there is some w in A so that

$$\lambda(y)\tau(x)\lambda(-y) = \tau(w).$$

Applying both sides to $z = 0$ in G gives $w = x - x \cdot y$. Then

$$\lambda(y)\tau(x)\lambda(-y)(z) = \tau(x - x \cdot y)(z)$$

is true for all x, y, z iff $x \cdot y \cdot z = 0$ for all x, y, z in A, iff $A^3 = 0$.

Finding the Hopf Galois structure

Let L/K be a Galois extension of fields with Galois group $G = (\mathbb{F}_p^n, +)$. Given A, a commutative nilpotent $\mathbb{F}_p$-algebra structure on the group G, with $A^3 = 0$. Let $T = \{\tau(x) : x \in G\}$ be the corresponding regular subgroup of $\mathrm{Perm}(G)$, acting on G by $\tau(x)(y) = x \circ y$.
Then the corresponding Hopf Galois structure on L/K is determined by:
i) the action of T on $GL = Hom_L(LG, L) = \sum_{y \in G} Le_y$ by

$$\tau(x)(e_y) = e_{x \circ y}.$$

Then GL/L is an LT-Hopf Galois extension of L
ii) the action of $\lambda(G)$ on T, by

$$\lambda(z)\tau(x)\lambda(-z) = \tau(x - x \cdot z).$$

Then L is a H-Hopf Galois extension of K where

$$H = (LT)^G$$

(descent)

In terms of the multiplication on A,

$$H = \{\sum_{x \in G} b_x \tau(x) | b_{x - x \cdot z} = b_x^z \text{ for all } z \text{ in } G\}$$

and H acts on L by

$$(\sum_{x \in G} b_x \tau(x))(a) = \sum_{x \in G} b_x a^{-x + x^2}.$$

$(-x + x^2) \circ x = 0)$

Examples of A with $n - r = 1$

Given a basis $x_1, \ldots, x_n$ for $G \cong (\mathbb{F}_p^n, +)$ we may identify $\mathrm{Hol}(G)$ with

$$\mathrm{Aff}_n(\mathbb{F}_p) = \begin{pmatrix} \mathrm{GL}_n(\mathbb{F}_p) & \mathbb{F}_p^n \\ 0 & 1 \end{pmatrix} \subset \mathrm{GL}_{n+1}(\mathbb{F}_p).$$

We look at a particularly nice class of commutative nilpotent algebras. Let A be a commutative nilpotent $\mathbb{F}_p$-algebra with $\dim(A) = n$, $\dim(A^2) = 1$, $A^3 = 0$. Choose a basis $(x_1, \ldots, x_{n-1}, x_n)$ with $A^2 = \langle x_n \rangle$. Then for all i, j,

$$x_i x_j = \phi_{i,j} x_n,$$

so A is determined by that basis and the single symmetric $n \times n$ structure matrix $\Phi = (\phi_{ij})$ satisfying

$$\overline{x}\overline{x}^T = \Phi x_n$$

(where $\overline{x}^T = (x_1, \ldots, x_n)$).

A regular subgroup from A

Since Φ is symmetric, there is a basis $\{z_j\}$ of A so that the structure matrix Φ of A relative to that basis is a diagonal matrix $D = \mathrm{diag}(d_1, \ldots, d_n)$ with $d_n = 0$.
Using that basis to identify $\mathrm{Hol}(G)$ with $\mathrm{Aff}_n(\mathbb{F}_p)$, the regular subgroup T corresponding to A is $T = \{\tau(\bar{r})\}$ where

$$\tau(\bar{r}) = \begin{pmatrix} I_{n-1} & 0 & \bar{r}_{n-1} \\ \bar{r}_d^T & 1 & r_n \\ 0 & 0 & 1 \end{pmatrix}$$

where $\bar{r}_{n-1}^T = (r_1, \ldots, r_{n-1})$, and $\bar{r}_d^T = (d_1 r_1, \ldots, d_{n-1} r_{n-1})$.
These regular subgroups and their conjugates under $\mathrm{GL}_n(\mathbb{F}_p)$ yield all the non-trivial regular subgroups for $n = 2$ and all but one orbit for $n = 3$.

Hopf Galois structures corresponding to A

To determine the number of Hopf Galois structures arising in that way from A, find the stabilizer of the regular subgroup T under conjugation by the elements of $\mathrm{Aut}(G) = \mathrm{GL}_n(\mathbb{F}_p)$.
For algebras A with $A^3 = 0$ and $\dim(A^2) = 1$ that is not difficult.

Start with a nice basis

We may choose a basis of A so that A has structure matrix

$$\Phi = \mathrm{diag}(D_s, 0)$$

where $D_s = \mathrm{diag}(1, \ldots, 1, s)$ is a $k \times k$ matrix with $s = 1$ or a non-square in $\mathbb{F}_p$. We may choose s to always be 1 if k is odd. So we have three cases.

Proposition. Let A be a commutative nilpotent $\mathbb{F}_p$-algebra of dimension n with $A^3 = 0$ and $\dim(A^2) = 1$. Suppose the structure matrix of A is $\Phi = \mathrm{diag}(D_s, 0)$ where D_s is $k \times k$ and

1) $k = 2m + 1, s = 1$

2) $k = 2m, s = 1$

3 $k = 2m$, s is a non-square in $\mathbb{F}_p$.

Then the number of distinct regular subgroups of $\mathrm{Aff}_n(\mathbb{F}_p)$ associated to A is

1)

$$\frac{|\mathrm{GL}_n(\mathbb{F}_p)|}{(\frac{p-1}{2}) \cdot |\mathrm{GO}_{2m+1}| \cdot |GL_{n-1-k}(\mathbb{F}_p)| \cdot p^{k(n-1-k)+(n-1)}}$$

2)

$$\frac{|\mathrm{GL}_n(\mathbb{F}_p)|}{(p-1) \cdot |\mathrm{GO}^+_{2m}| \cdot |GL_{n-1-k}(\mathbb{F}_p)| \cdot p^{k(n-1-k)+(n-1)}}$$

3)

$$\frac{|\mathrm{GL}_n(\mathbb{F}_p)|}{(p-1) \cdot |\mathrm{GO}^-_{2m}| \cdot |GL_{n-1-k}(\mathbb{F}_p)| \cdot p^{k(n-1-k)+(n-1)}}$$

$n = 2, 3, 4$

For $n = 2, 3$ these agree with results obtained previously (e.g. in [Ch05] for $n = 3$).
For $n = 4$ there are four subcases. As above, s is a non-square in $\mathbb{F}_p$.

(d_1, d_2, d_3)	number of regular subgroups
$(1, 0, 0)$	$(p^2 + 1)((p + 1)(p^3 - 1)$
$(1, 1, 0)$	$p(p^2 + 1)(p + 1)(p^3 - 1)(p + 1)/2$
$(1, s, 0)$	$p(p^4 - 1)(p^3 - 1)/2$
$(1, 1, 1)$	$p^2(p^4 - 1)(p^3 - 1)$

The sum exceeds p^9.

Connections to Galois module theory?

Suppose L/K is Galois with group G elementary abelian of order p^2. In that setting it is well known that there are $p^2 - 1$ non-classical Hopf Galois structures on L/K. [By02] describes them as follows.
Pick a subgroup $\langle\tau\rangle \subset G$ of order p and let $G = \langle\sigma, \tau\rangle$. Define the regular subgroup $J_{d,\tau} = \langle\rho, \mu\rangle$ of $\mathrm{Perm}(G)$ by

$$\rho(\sigma^k\tau^l) = \sigma^k\tau^{l-1}$$
$$\mu(\sigma^k\tau^l) = \sigma^{k-1}\tau^{l+dk-d}$$

for $d = 0, 1, \ldots, p-1$. For $d = 0$ one recovers the classical Hopf Galois structure. For $d \neq 0$, every $J_{d,\tau}$ is normalized by $\lambda(G)$, hence the group ring $LJ_{d,\tau}$ descends to a K-Hopf algebra that yields a Hopf Galois structure on L/K.
So there are $p-1$ non-classical Hopf Galois structures for each of the $p+1$ choices of the order p subgroup $\langle\tau\rangle$ of G.

[By02]

Now suppose L/K is totally ramified with break numbers

$$pj - 1 = t_1 < t_2 = p^2 i - 1.$$

Let G_{t_2} be the corresponding ramification group of order p. Then [By02] showed

• If $t_1 < t_2$ and $\mathfrak{O}_L$ is Hopf Galois over $\mathfrak{O}_K$ with respect to a Hopf order in $H_{d,\tau}$, then $\langle \tau \rangle$ must $= G_{t_2}$.

• If $j < pi$ and $i \geq 2j$, then $\mathfrak{O}_L$ is Hopf Galois over $\mathfrak{O}_K$ for a Hopf order in $H_{d,\tau}$ for a unique d, and $H_{d,\tau}$ is non-classical (that is, $d \neq 0$) if and only if $(p+1)j = pi + 1$.

Our regular subgroups

The regular subgroup T_A of $\mathrm{Aff}_2(\mathbb{F}_p)$ obtained from the nilpotent $\mathbb{F}_p$-algebra $A = \langle x_1, x_2 \rangle$ with $x_1^2 = x_2$ is

$$T_A = \left\langle \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle$$

$$= \left\{ \begin{pmatrix} 1 & 0 & r_1 \\ r_1 & 1 & r_2 \\ 0 & 0 & 1 \end{pmatrix} \right\}$$

with respect to the basis (x_1, x_2) of G. We get $p^2 - 1$ others by conjugating T_A by $\begin{pmatrix} P & 0 \\ 0 & 1 \end{pmatrix}$ where P is in $\mathrm{GL}_2(\mathbb{F}_p)$.

The group $J_{d,\tau}$

We can embed Byott's group $J_{d,\tau}$ in $\mathrm{Aff}_2(\mathbb{F}_p)$ where $\sigma = x_1, \tau = x_2$ by

$$\rho = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}, \mu = \begin{pmatrix} 1 & 0 & -1 \\ d & 1 & -d \\ 0 & 0 & 1 \end{pmatrix}.$$

For $d \neq 0$ and e with $de = 1$,

$$\mathrm{diag}(1, e, 1) J_{d,\tau} \mathrm{diag}(1, d, 1) = T_A.$$

So Byott's regular subgroups are conjugates of our group T_A.

Guidance from Byott

[By02] says that for doing Galois module theory, choose the basis x_1, x_2 for constructing A so that x_2 generates the ramification group G_{t_2} of order p.

If we then conjugate $J_{d,\tau}$ by $\begin{pmatrix} P^{-1} & 0 \\ 0 & 1 \end{pmatrix}$, the resulting regular subgroup is J_{f,y_2} where $P\binom{0}{1}$ are the coordinates of y_2 relative to the basis (x_1, x_2). Thus, to preserve the ramification group $\langle x_2 \rangle$, P must be lower triangular. (For $n = 2$ we may as well assume P is diagonal.)

Which Hopf Galois structures might be useful?

For general n, we should start with a basis for G that corresponds to the ramification filtration of G. Given a commutative nilpotent algebra A with a nice multiplication using that basis, the interesting regular subgroups should be conjugates of the corresponding regular subgroup T_A by elements of $\mathrm{GL}_n(\mathbb{F}_p)$ that respect the ramification filtration of G.

In particular, if G has n distinct ramification group, one should restrict interest to regular subgroups obtained from T_A by conjugating by lower triangular matrices P.

That significantly reduces the number of relevant Hopf Galois structures associated to a commutative nilpotent algebra A: for example, for $n = 2$, from $p^2 - 1$ to $p - 1$.

When $\dim(A^2) = 1$

Let A be a commutative nilpotent algebra A with $\dim(A^2) = 1, A^3 = 0$ and suppose that relative to a basis that respects the ramification filtration, the structure matrix $\Phi = \mathrm{diag}(D_s, 0)$ with D_s $k \times k$. Let T_A be the corresponding regular subgroup. How many distinct regular subgroups do we get by conjugating by lower triangular automorphisms P? by diagonal automorphisms P?
Proposition: Let L/K of dimension p^n have n distinct break numbers. Then the number of distinct regular subgroups that respect the ramification filtration of L/K, is

$$= 2(\frac{p-1}{2})^k p^{\frac{(k-1)k}{2}}.$$

If we restrict to diagonal automorphisms, then the number

$$= 2(\frac{p-1}{2})^k.$$

These numbers depend only on k (and not on n). For $k = 1$ we obtain $p - 1$, which in particular yields Byott's result for $n = 2$.

Extending [By02] to $n = 3$?

To finish up, it appears that to extend [By02] to the case $n = 3$, one needs
1. a complete description of Hopf Galois structures on L/K with Galois group G.
For $p > 3$ all five isomorphism types of commutative nilpotent $\mathbb{F}_p$-algebras A of dimension 3 satisfy $A^p = 0$, hence yield Hopf Galois structures of type G. So they all yield distinct orbits of regular subgroups of $\mathrm{Aff}_3(\mathbb{F}_p)$. One orbit is that of $\lambda(G)$, and three others arise from A with $\dim(A^2) = 1$:

$$\Phi = \mathrm{diag}(1, 0, 0), \Phi = \mathrm{diag}(1, 1, 0), \Phi = \mathrm{diag}(1, s, 0).$$

They each yield Hopf Galois structures directly, as in [By02], without translating from the holomorph, and we just described number of Hopf Galois structures that preserve the ramification filtration when there are three distinct break numbers.

The other is the algebra $A_J = \langle x \rangle$ with $x^4 = 0$. The corresponding regular subgroups of $\mathrm{Aff}_3(\mathbb{F}_p)$ corresponding to A_J are not normalized by $\lambda(G)$, so one has to translate from the holomorph to $\mathrm{Perm}(G)$. That is doable but not as clean as the other cases.

Hopf Galois structure plus...

But then one also needs:

2. a complete description of Hopf orders, in particular, realizable orders, in the K-Hopf algebras of K-dimension 3 arising from the Hopf Galois structures.

As the conference showed, this remains work in progress. So

3. a nice criterion (e.g. a congruence condition) to match up the extension L/K with a suitable Hopf order.

is not available either.

Acknowledgement

This work was inspired by a remark by Tim Kohl that for G commutative a good many regular subgroups of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$ can be found in $\mathrm{Hol}(G)$.

Many thanks to Nigel, Griff and Henri for an excellent conference, and for inviting me.

References

[By96] .N. P. Byott, Uniqueness of Hopf Galois structure of separable field extensions, Comm. Algebra 24 (1996), 3217–3228.

[By00] .N. P. Byott, Galois module theory and Kummer theory for Lubin-Tate formal groups, pp 55–67 in "Algebraic Number Theory and Diophantine Analysis" (F Halter-Koch, R Tichy, eds), (Proceedings of Conference in Graz, 1998), Walter de Gruyter, 2000.

[By02] .N. P. Byott, Integral Hopf-Galois structures on degree p^2 extensions of p-adic fields, J. Algebra, 248, (2002), 334–365.

[By04] .N. P. Byott, Hopf-Galois structures on field extensions with simple Galois groups, Bull. London Math. Soc. 36 (2004), 23–29.

[BC12] .N. P. Byott, L. N. Childs, Fixed-point free pairs of homomorphisms and nonabelian Hopf-Galois structure, New York J. Math. 18 (2012), 707–731.

[CaC99] .S. Carnahan, L. N. Childs, Counting Hopf Galois structures on non-abelian Galois field extensions. J. Algebra 218 (1999), 81–92.

[Ch03] .L. N. Childs, On Hopf Galois structures and complete groups, New York J. Mathematics 9 (2003) 99–116.

[Ch05] .L. N. Childs, Elementary abelian Hopf Galois structures and polynomial formal groups, J. Algebra 283 (2005), 292–316.
[Ch15] .L. N. Childs, On Abelian Hopf Galois structures and finite commutative nilpotent rings, New York J. Math., 21 (2015), 205–229.

[FCC12] .S. C. Featherstonhaugh, A. Caranti, L. N. Childs, Abelian Hopf Galois structures on prime-power Galois field extensions, Trans. Amer. Math. Soc. 364 (2012), 3675–3684.

[GP87] . C. Greither, B. Pareigis, Hopf Galois theory for separable field extensions, J. Algebra 106 (1987), 239–258.

[KP70] .R. L. Kruse, D. T. Price, Enumerating finite rings, J. London Math. Soc. (2), 2 (1970), 149–159.

[Po08a] . B. Poonen, The moduli space of commutative algebras of finite rank, J. Europ. Math. Soc. 10 (2008), no. 3, 817–836.

[Po08b] . B. Poonen, Isomorphism types of commutative algebras of finite rank over an algebraically closed field, Computational Arithmetic Geometry (edited by K. Lauter and K. Ribet), Contemporary Math. 463 (2008), Amer. Math. Soc., 111–120.