QUANTIFYING FAILURE OF THE FTGT FOR CERTAIN HOPF GALOIS STRUCTURES

LINDSAY CHILDS

0.1. **Introduction.** Let L/K be a Galois extension with Galois group Γ an elementary abelian p group of order p^n. Suppose L/K also has an H-Hopf Galois structure of type $G \cong \Gamma$. In my talk last year I showed that the Galois correspondence from K-subHopf algebras of H to intermediate fields was surjective if and only if the Hopf Galois structure is the classical structure by the Galois group Γ. What I want to do today is to try to quantify the failure of the FTGT in this setting.

This work is joint with Cornelius Greither. It arose from conversations we had after my talk here last year.

0.2. **Caranti, della Volta, Sala.** Let G be a finite abelian group of order p^n, written additively. Let $\lambda : G \to \mathrm{Perm}(G)$ be the left regular representation, $\lambda(g)(h) = g + h$. The normalizer in $\mathrm{Perm}(G)$ of $\lambda(G)$ is $\mathrm{Hol}(G) = \lambda(G) \cdot \mathrm{Aut}(G)$, the holomorph of G.

Let $A = (G, +, \cdot)$ be a commutative nilpotent ring (without unit), or radical ring, with additive group G. Define the circle operation $\circ : G \times G \to G$ by

$$a \circ b = a + b + a \cdot b.$$

Define a map $\tau : (G, \circ) \to \mathrm{Perm}(G)$ by $\tau(a)(g) = a \circ g$. Then τ is a one-to-one homomorphism, whose image $T = \tau(G)$ is a regular subgroup of $\mathrm{Perm}(G)$ ($\tau(G)(0) = G$), and is contained in $\mathrm{Hol}(G)$.

This map from commutative nilpotent ring structures on $(G, +)$ to commutative regular subgroups of $Hol(G)$ is bijective, by work of Caranti, della Volta and Sala. That is, every commutative regular subgroup of $\mathrm{Hol}(G)$ is the image of the circle group of some commutative nilpotent ring structure on $(G, +)$.

0.3. Now specialize to the case where $G = (\mathbb{F}_p^n, +)$ is elementary abelian under addition, and we only consider commutative nilpotent ring structures $A = (G, +, \cdot)$ where $A^p = 0$. Then $(G, \circ)$ will also be an elementary abelian p-group.

Date: Omaha, May 2017.

Let L/K be a Galois extension of fields with Galois group Γ where Γ is an elementary abelian p-group of order p^n. Let $T = \tau(G, \circ)$ be an elementary abelian regular subgroup of $\mathrm{Hol}(G)$, coming from a commutative nilpotent $\mathbb{F}_p$-algebra structure A on $(G, +)$. Let $\beta : \Gamma \to T$ be an isomorphism. Then corresponding to β is an embedding $\alpha : G \to \mathrm{Perm}(\Gamma)$, whose image N is normalized by $\lambda(\Gamma)$. So N corresponds to an H-Hopf Galois structure on L/K, where $H = (LN)^\Gamma$ (Γ acts on L via the action by the Galois group and on N by conjugation by $\lambda(\Gamma)$ in $\mathrm{Perm}(\Gamma)$).

To examine the FTGT for the H-Hopf Galois structure on L/K we compare the number of K-subHopf algebras of H to the number of intermediate fields E with $K \subseteq E \subseteq L$.

0.4. The main result of [Ch17]. Since L/K is classically Galois with Galois group $\Gamma \cong (\mathbb{F}_p^n, +)$, the classical FTGT holds for L/K, so the number of intermediate fields is equal to the number of subgroups of Γ, $= s(n)$, the number of subspaces of $\mathbb{F}_p^n$.

From [Ch17], the number of K-subHopf algebras of H is equal to the number of ideals of the commutative nilpotent $\mathbb{F}_p$-algebra $A = (\mathbb{F}_p^n, +, \cdot)$ corresponding to the K-Hopf Galois structure on L/K.

The number of ideals of A is equal to the number of subspaces of A if and only if the multiplication on A is trivial ($ab = 0$ for all a, b in A), if and only if the Hopf Galois structure by H is the classical structure given by the Galois group Γ. So for all other Hopf Galois structures (for Γ elementary abelian), the FTGT fails.

0.5. Our question. How badly does the FTGT fail?

To try to answer that question, we take a commutative nilpotent $\mathbb{F}_p$-algebra of $\mathbb{F}_p$-dimension n and ask, what can we say about $i(A)$, the number of ideals of A? How does it compare with $s(A)$, the number of subspaces of A?

Let

$$\begin{aligned} \delta(t) &= \frac{t^2}{4} \text{ if } t \text{ is even} \\ &= \frac{t^2 - 1}{4} \text{ if } t \text{ is odd} \end{aligned}$$

If $\dim_{\mathbb{F}_p} A = n$, then $s(A) = s(n)$. We know that $s(n) \geq p^{\delta(n)}$ and is a polynomial in p of degree $\delta(n)$.

0.6. Our main result. Let A be a (commutative) nilpotent $\mathbb{F}_p$-algebra of dimension n. Then $A^{n+1} = 0$. Let $e > 0$ be minimal with $A^{e+1} = 0$.

Theorem 0.1. *Let A be a commutative nilpotent $\mathbb{F}_p$-algebra A with $A^{e+1} = 0$. Then*

$$i(A) \leq \frac{2e-1}{p^{\delta(e)}} s(A).$$

0.7. A consequence for Hopf Galois structures. The upper bound is of particular interest in the form

$$\frac{i(A)}{s(A)} \leq \frac{2e-1}{p^{\delta(e)}}.$$

Recall that $\delta(e) = \lfloor \frac{e^2}{4} \rfloor \geq 1$ for $e \geq 2$. So for $e \geq 2$, as p increases, the ratio of ideals to subspaces approaches zero.

Corollary.

$$\frac{i(A)}{s(A)} < .01$$

for

- $e = 2$, $p \geq 300$
- $e = 3$, $p \geq 25$
- $e = 4$, $p \geq 7$
- all e, p with $5 \leq e < p$.

0.8. The upper bound strategy. The idea is the following. Let

$$G : \{\text{subspaces of } A\} \to \{\text{ideals of } A\}$$

be the "ideal generated by" map. We ask: how big are the fibers $G^{-1}(J)$ for J an ideal of A? How many subspaces of J generate J?

The answer depends on where the ideal sits in A.

0.9. A chain of annihilator ideals. Consider the chain

$$\{0\} = N_0 \subset N_1 \subset N_2 \subset \ldots \subset N_e = A$$

of annihilator ideals defined by

$$N_k := \mathrm{Ann}_k(A) = \{a \in A | x_1 x_2 \cdots x_k a = 0 \text{ for all } x_1, \ldots x_k \text{ in } A\}.$$

For example. If $J \subset N_1$, then $G^{-1}(J) = \{J\}$, because every subspace of $N_1 = Ann_1(A)$ is an ideal of A. So $|G^{-1}(J)| = 1$.

On the other hand, the ideal $N_e = A$ itself is generated by at least $p^{\delta(n)}$ subspaces.

0.10. Principal ideals. To get our inequality, we look at principal ideals. We first observe:

Lemma: let $J = G(\langle x \rangle) = \mathbb{F}_p x + Ax$ and let $W_0 = Ax$. Then every subspace U of J not contained in W_0 contains x, so generates J.

Let $\dim J = q$. Then the number of subspaces U of J not contained in W_0 is at least $p^{\delta(q)}$ (a linear algebra exercise). So:

For J a principal ideal of dimension q, $|G^{-1}(J)| \geq p^{\delta(q)}$.

0.11. Stratifying ideals. To get an lower bound on $q = \dim(J)$ for J a principal ideal, we look at ideals J contained in N_t, not contained in N_{t-1}.

Lemma: For each t, and each x in $N_t \backslash N_{t-1}$, let $q(x)$ be the dimension of $G(\{x\})$, and let q_t be the minimum of $q(x)$ for all x in $N_t \setminus N_{t-1}$. Then $q_t \geq t$.

The idea is that if x is in N_t and not in N_{t-1}, then there is a sequence of elements $a_1 \ldots, a_{t-1}$ in A so that $a_1 a_2 \cdots a_{t-1} x \neq 0$. Letting $x_i = a_1 a_2 \cdots a_i x$, each x_i is not in $N_{t-(i+1)}$ but is in N_{t-i}. So $x, x_1, \ldots, x_{t-1}$ are linearly independent elements of $G(\{x\})$.

0.12. Let $\mathcal{J}_t$ be the set of ideals J contained in N_t, not contained in N_{t-1}.

For J in $\mathcal{J}_t$, J contains an element x in N_t, not in N_{t-1}, hence contains the principal ideal generated by x. So

Proposition: For J an ideal contained in N_t, not in N_{t-1}, the number of subspaces that generate J is at least $p^{\delta(q_t)}$, where q_t is the minimum of the dimensions of principal ideals generated by x in N_t, not in N_{t-1}.

0.13. Counting. Since N_t is an ideal, every subspace of N_t generates an ideal that is contained in N_t. So we have

$$\sum_{J \in \mathcal{J}_t} |G^{-1}(J)| = s(N_t) - s(N_{t-1}).$$

Now $|\mathcal{J}_t| = i(N_t) - i(N_{t-1})$.

For J in $\mathcal{J}_t$, we observed that

$$|G^{-1}(J)| \geq p^{\delta(q_t)}$$

where q_t is the minimum dimension of principal ideals in N_t, not in N_{t-1}. So replacing $|G^{-1}(J)|$ by $p^{\delta(q_t)}$ in our equation above gives

$$p^{\delta(q_t)}(i(N_t) - i(N_{t-1})) \leq s(N_t) - s(N_{t-1}).$$

0.14.

$$p^{\delta(q_t)}(i(N_t) - i(N_{t-1})) \leq s(N_t) - s(N_{t-1}).$$

Dividing by $p^{\delta(q_t)}$ and summing over all t gives an upper bound for $i(A)$:

$$i(A) \leq \sum_{t=1}^{e-1}(p^{-\delta(q_t)} - p^{-\delta(q_{t+1})})s(N_t) + p^{-\delta(q_e)}s(N_e).$$

0.15. Completing the upper bound. To clean this up, we apply the following general result connecting $s(m)$ and $s(n)$: For $n \geq m \geq 0$ arbitrary,

$$s(n) \geq \frac{1}{2}p^{\delta(n)-\delta(m)}s(m).$$

Using that and the inequality $q_t \geq t$ yields our upper bound

$$i(A) \leq \frac{2e-1}{p^{\delta(e)}}s(A),$$

0.16. A lower bound on ideals? To get a more precise idea of the size of the image of the Galois correspondence map for the Hopf Galois structures we're looking at, we seek a lower bound on $i(A)$.

0.17. A lower bound. Recall that N_k is the k-th annihilator ideal of A,

$$N_k = \{a \in A | x_1x_2 \cdots x_kx = 0 \text{ for all } x_1, \ldots x_k \in A\}.$$

Let $\dim_{\mathbb{F}_p}(N_k) = d_k$. Then $0 < d_1 < d_2 < \ldots < d_e = n$. Let $t_k = d_k - d_{k-1}$, and let $t_M = \max_k t_k$. Then we have:

Theorem 0.2. *$i(A) \geq \lambda(A)$, where*

$$\lambda(A) = s(t_1) + s(t_2) + \ldots + s(t_e) - (e-1).$$

0.18. Counting some ideals. We get the lower bound on $i(A)$ by identifying some ideals and counting them.

The chain of annihilator ideals is

$$\{0\} = N_0 \subset N_1 \subset N_2 \subset \ldots \subset N_e = A.$$

Let W_k be a subspace of A so that $N_k = W_k \oplus N_{k-1}$. Then $\dim(W_k) = t_k = d_k - d_{k-1}$ and

$$A = W_1 \oplus W_2 \oplus \ldots \oplus W_e.$$

For V_k any subspace of W_k, the space $V_k \oplus N_{k-1}$ is an ideal of A, because N_{k-1} is an ideal of A and $aV_k \subset aN_k \subseteq N_{k-1}$ for all a in A.

Omitting the case $V_k = 0$ except when $k = 0$ gives us $s(W_k) - 1 = s(t_k) - 1$ ideals. So the number of ideals counted is

$$\lambda(A) = s(t_1) + s(t_2) + \ldots + s(t_e) - (e-1).$$

For some A the lower bound is pretty good, as we'll see.

0.19. An example. Let $A = \langle x \rangle$ with $x^{e+1} = 0$. Then $\dim(A) = e$.

The lower bound $\lambda(A) = e + 1$ since $t_i = 1$ for all i, and $s(1) = 2$.

As for the upper bound, note that $s(e)$ is a polynomial in p of degree $p^\delta(e)$ with leading coefficient 1 or 2 (depending on whether e is even or odd), so in the upper bound

$$i(A) \leq \frac{2e-1}{p^{\delta(e)}} s(A) = \frac{2e-1}{p^{\delta(e)}} s(e),$$

the ratio

$$\frac{(2e-1)s(e)}{p^{\delta(e)}} \longrightarrow 2e-1 \text{ or } 2(2e-1)$$

as $p \to \infty$.

In fact, $i(A) = e+1$. So the lower bound is sharp and, since $\dim(A) = e$, the upper bound for large p converges to a constant not much larger than $i(A)$.

0.20. A binomial example. Let A be the binomial algebra of dimension 15,

$$A = \langle x_1, x_2, x_3, x_4 \rangle$$

with $x_i^2 = 0$. Then

$$\begin{aligned} N_1 &= \langle x_1x_2x_3x_4 \rangle, \\ N_2 &= \langle x_1x_2x_3, x_1x_2x_4, x_1x_3x_4, x_2x_3x_4 \rangle, \\ N_3 &= \langle x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_4, x_3x_4 \rangle, \\ N_4 &= \langle x_1, x_2, x_3, x_4 \rangle = A \end{aligned}$$

Then $e = 4$. Our inequalities for $i(A)$ yield

$$\lambda(A) \leq i(A) \leq \frac{7}{p^{\delta(4)}} s(15).$$

0.21.

$$\lambda(A) \leq i(A) \leq \frac{7}{p^{\delta(4)}} s(15),$$

Now the lower bound $\lambda(A)$ satisfies

$$p^9 < s(6) < \lambda(A) = s(1) + s(4) + s(6) + s(4) - 3 < p^{10}$$

for $p \geq 3$, and since $p^{56} < 7s(15) < p^{57}$ for large p and $\delta(4) = 4$, we have

$$p^9 \leq i(A) \leq p^{53}.$$

So for this example (and others), our upper and lower bounds for $i(A)$ are not close to each other.

0.22. Tweaking the upper bound. For some classes of examples of algebras, the dimensions of principal ideals inside N_t, not in N_{t-1} are bounded by $q_t > t$.

For example, for a binomial algebra, every principal ideal in N_t, not in N_{t-1}, has dimension at least 2^{t-1}. Using this for our binomial example of dimension 15 lowers the upper bound on $i(A)$ from p^{53} to p^{41}. Still not very good.

0.23. A smaller example. I spent some time on examples, trying to actually count the number of ideals.

Consider the triangular algebra $A = \langle x, y\rangle$ with $A^3 = 0$ and basis (x, y, x^2, xy, y^2). So $e = 2$.

The lower bound is

$$2p^2 + 3p + 6 \leq i(A).$$

The upper bound is

$$i(A) \leq \frac{3}{p}s(5) = \frac{3}{p}(2p^6 + 2p^5 + 6p^4 + 6p^3 + 6p^2 + 4p + 6).$$

The actual number of ideals is

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

0.24. Why is the upper bound so off? The issue is that our method assumed that every ideal J contained in N_t, not in N_{t-1} has dimension the size of a principal ideal J with the same properties. But that is not so. In this example, we have the following ideals:

$$\begin{aligned}
&A = G(x, y)\\
&J_1(a, d) = G(x + ay + dy^2)\\
&J_{15}(a) = G(x + ay, y^2)\\
&J_2(b) = G(y + bx^2)\\
&J_{23} = G(y, x^2)\\
&\text{ideals of } N_1
\end{aligned}$$

(where a, d, b are parameters from $\mathbb{F}_p$).

0.25. The number of ideals of each type and the number of subspaces that generate each ideal of the given type is given by the table:

ideals	# of ideals	fiber size
A	1	$2p^6+p^5+2p^4+p^3+p^2+1$
$J_1(a,d)$	p^2	$2p^2+p+1$
$J_{15}(a)$	p	$p^4+p^3+p^2+1$
$J_2(b)$	p	$2p^2+p+1$
J_{23}	1	$p^4+p^3+p^2+1$
ideal of N_1	$2p^2+2p+4$	1

The p^2+p principal ideals $J_1(a,d)$ and $J_2(b)$ are each generated by $2p^2+p+1$ subspaces. The $p+1$ non-principal ideals J_{23} and $J_{15}(a)$ are each generated by $p^4+p^3+p^2+1$ subspaces. And the ideal A itself is generated by $2p^6+p^5+2p^4+p^3+p^2+1$ subspaces. So our upper bound on $i(A)$ is weak because we considerably undercounted the fibers of the non-principal ideals.

0.26. The binomial algebra on three generators. We did a similar analysis for the binomial algebra of dimension 7, with three generators ($e=3$). It has $\sim p^{12}$ subspaces. Our lower bound is

$$\lambda(A) = 4p^2+4p+8.$$

The number of ideals is

$$i(A) = 7p^2+4p+8,$$

while our best upper bound based on the dimensions of principal ideals is

$$\frac{2}{p^{-4}}s(A) = 4p^8+2p^7+\dots.$$

For this example, the number of subspaces of A is

$$s(A) = s(7) = 2p^{12}+2p^{11}+6p^{10}+8p^9+\dots,$$
$$G^{-1}(A) = 2p^{12}+p^{11}+2p^{10}+2p^9+\dots,$$

the fibers of the p^2+p+1 non-principal ideals not contained in N_2 account for $\sim p^{11}$ subspaces, and the remaining ideals account for $\sim p^8$ subspaces.

0.27. Conclusion. So for an algebra A with $A^e \neq 0, A^{e+1}=0$, undercounting the subspaces that generate non-principal ideals not contained in A^{e-1} seeems to be the chief culprit in the weakness of the upper bound. If we could more effectively count the sizes of non-principal ideals and integrate them into a formula like

$$\sum_{J\in\mathcal{J}_t} |G^{-1}(J)| = s(N_t)-s(N_{t-1}),$$

we would likely have a better upper bound on $i(A)$. But...

0.28. Bottom line. The upper bound on ideals that we found is good enough to show how badly the FTGT fails for Hopf Galois structures on elementary abelian Galois extensions L/K of order p^n.

0.29. Caveat. I found this comment on the study of nilpotent algebras:

From "The Theorem of Wedderburn-Malcev..." by Rolf Farnsteiner: https://www.math.uni-bielefeld.de/ sek/select/RF6.pdf

"Throughout, A denotes a finite dimensional algebra over a field k. We let Rad(A) be the Jacobson (nilpotent) radical of A. Wedderburns classical result tells us that the semisimple factor algebra A/ Rad(A) is a direct sum of matrix algebras ...

"To understand the structure of A, two problems remain, namely,

- the determination of the structure of Rad(A), and
- the interaction of the constituents A/ Rad(A) and Rad(A).

The former usually is a hopeless endeavor...."

0.30. Play. Some examples to play with:

- Poonen's list of isomorphism types of local nilpotent algebras of dimension ≤ 5
- binomial algebras
- "triangular" algebras $A = \langle x, y\rangle$ with $A^{e+1} = 0$
- generalized triangular algebras $A = \langle x_1, x_2, \dots x_r\rangle$ with $A^{e+1} = 0$,
- truncated diagonal algebras $A = \langle x, y\rangle$ with $x^n = y^m = 0$.
- More generally, algebras A in which all relations are monomials (such as the last four examples and 14 of Poonen's 25 examples of dimension 5 for $p \geq 3$).

Thank you.