APPLICATIONS OF NILPOTENT ALGEBRAS TO HOPF GALOIS STRUCTURES

LINDSAY N. CHILDS

Abstract. Let L/K be a Galois extension of fields with Galois group G, an elementary abelian p-group of order p^n, p an odd prime. For $n > 1$, L/K has non-classical Hopf Galois structures of type G, which have been studied by looking at regular subgroups of $\mathrm{Hol}(G)$ that are isomorphic to G. Think of G as an additive group $(G, +)$. This talk exploits the connection, introduced by Caranti, Della Volta and Sala in 2006, between regular subgroups of $\mathrm{Hol}(G)$ and associative, commutative nilpotent algebra structures A on $(G, +)$. We briefly review three known consequences of this connection for Hopf Galois structures. Then we describe how the connection helps understand the lack of surjectivity of the Galois correspondence from subHopf algebras to subfields given by the Chase-Sweedler Fundamental Theorem of Galois Theory for a Hopf Galois structure on L/K.

This is the text of a presentation at the workshop on Hopf Algebras and Galois Module Theory held at the University of Nebraska at Omaha, May 23, 2016.

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 $j : L \otimes_K H \to End_K(L)$ given by $j(s \otimes h)(t) = sh(t)$ is a bijection.

If L/K is a Galois extension with Galois group Γ, then L/K is a $K\Gamma$-Hopf Galois extension.

Assume that L/K is a Galois extension of fields with Galois group Γ, an elementary abelian p-group of order p^n.

If L/K is also an H-Galois extension, then tensoring over K with L yields an action

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

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

This begins a sequence of correspondences:

Date: June 9, 2016.

Three correspondences.

{Hopf Galois structures on L/K by K-Hopf algebras H of type $G \cong \Gamma$}

[GP87] $\updownarrow$

{ regular subgroups N of $\mathrm{Perm}(\Gamma)$ normalized by $\lambda(\Gamma)$ }

[By96] $\updownarrow$

{Regular embeddings $\beta : \Gamma \to \mathrm{Hol}(G)$ up to equivalence }

[CDVS06] $\updownarrow$

{Nilpotent (associative, commutative) algebra structures A on $(G, +)$ with $A^p = 0$ up to isomorphism}.

The first correspondence. The first correspondence is the main result of Greither and Pareigis [GP87]. For

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

where $\{e_\gamma : \gamma \in \Gamma\}$ is a dual basis to the elements γ of Γ. Then([GP87]) $L \otimes_K H$ is a group ring LN where $N \subset \mathrm{Perm}(\Gamma)$ acts on ΓL as a regular group of permutations of the dual basis of Γ, and is normalized by the image $\lambda(\Gamma)$ of the left regular representation of Γ in $\mathrm{Perm}(\Gamma)$.

The correspondence is bijective, because given a regular subgroup N of $\mathrm{Perm}(\Gamma)$ normalized by $\lambda(\Gamma)$, the regularity of N implies that the action of LN on ΓL makes the extension $\Gamma L/L$ into an LN-Hopf Galois extension. Since N is normalized by $\lambda(\Gamma)$, Galois descent of the Hopf Galois extension over L (that is, taking fixed subrings under the action of Γ acting on L by the action of the Galois group of L/K and on N by conjugation by $\lambda(\Gamma)$) yields a K-Hopf algebra H and an action of H on L making L a Hopf Galois extension of K. If we start with a Hopf Galois structure of H on L over K, base change to L and then descend, we recover the given Hopf Galois structure on L/K.

The type of H. Let N be a regular subgroup of $\mathrm{Perm}(\Gamma)$ normalized by $\lambda(\Gamma)$. Then N has the same order as $\lambda(\Gamma)$. Let G be an abstract group of the same cardinality as Γ and $\alpha : G \to N$ be an isomorphism. Then the corresponding K-Hopf algebra H has *type* G. Viewing N as a subgroup of $\mathrm{Perm}(\Gamma)$, the map $\alpha : G \to N$ is a regular embedding of G in $\mathrm{Perm}(\Gamma)$.

The second correspondence. As shown in [By96], a regular embedding $\alpha : G \to \mathrm{Perm}(\Gamma)$ whose image $\alpha(G)$ is normalized by $\lambda(\Gamma)$ corresponds to a regular embedding $\beta : \Gamma \to \mathrm{Hol}(G)$, where

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

is the normalizer of $\lambda(G)$ in $\mathrm{Perm}(G)$. Here $\rho : G \to \mathrm{Perm}(G)$ is the right regular representation of G in $\mathrm{Perm}(G)$. The relationship between α and β is as follows:

How $\alpha \longleftrightarrow \beta$ works. Let $\beta : \Gamma \to \mathrm{Hol}(G)$ be a regular embedding. Define $b : \Gamma \to G$ by

$$b(\gamma) = \beta(\gamma)(e_G)$$

for γ in Γ, where e_G is the identity element of G. Then b is an identity-preserving bijection, and b recovers β: for all g in G,

$$\beta(\gamma)(g) = (b(\lambda(\gamma))b^{-1})(g) = (C(b)\lambda(\gamma))(g)$$

Define $\alpha : G \to \mathrm{Perm}(\Gamma)$ by

$$\alpha(g)(\gamma) = (b^{-1}(\lambda(g))b)(\gamma) = (C(b^{-1})\lambda(g))(\gamma).$$

Then $\alpha(g)(e_\Gamma) = b^{-1}(g)$ and $C(b)\lambda(\gamma) = \beta$. Then $\alpha(G)$ is normalized by $\lambda(\Gamma)$. In fact,

Proposition 1. *Suppose $\beta : \Gamma \to \mathrm{Hol}(\lambda(G))$ is an regular embedding, and let $\alpha = C(b^{-1})\lambda_G : G \to \mathrm{Perm}(\Gamma)$ be the regular embedding corresponding to β. Then for all γ in Γ and g in G, there is some h in G so that*

$$\beta(\gamma)\lambda(g)\beta(\gamma)^{-1} = \lambda(h)$$

and

$$\lambda(\gamma)\alpha(g)\lambda(\gamma)^{-1} = \alpha(h).$$

Proof. The first formula follows because β maps Γ into $\mathrm{Hol}(G)$, the normalizer of $\lambda(G)$ in $\mathrm{Perm}(G)$. Since $C(b^{-1})(\beta)(\gamma) = \lambda(\gamma)$ and $C(b^{-1})\lambda(g) = \alpha(g)$, the second formula follows from the first by applying $C(b^{-1})$ to the first formula. $\square$

The third correspondence. The third correspondence comes from Caranti, et. al., [CDVS06], [FCC12].

Proposition 2. *Let $(G,+)$ be a finite abelian p-group. Then each regular subgroup of* Hol(G) *is isomorphic to the group $(G,\circ)$ induced from a structure $(G,+,\cdot)$ of a commutative, associative nilpotent ring (hereafter, "nilpotent") on $(G,+)$, where the operation $\circ$ is defined by $g\circ h = g+h+g\cdot h$.*

The idea is the following: Let $(G,+)$ be an abelian group of order p^n , and suppose that $A=(G,+,\cdot)$ is a nilpotent ring structure on $(G,+)$ yielding the operation $\circ$. Define $\tau : (G,\circ) \to \mathrm{Perm}(G,+)$ by $\tau(g)(x) = g\circ x$. Then $\tau(g)(0) = g$, and

$$\tau(g)\tau(g')(x) = \tau(g)(g'\circ x) = g\circ(g'\circ x) = (g\circ g')\circ x = \tau(g\circ g')(x).$$

Thus τ is a regular embedding of $(G,\circ)$ into $\mathrm{Perm}(G,+)$. Since A is nilpotent, $(G,\circ)$ is a group, for $a\circ(-a+a^2-a^3+\ldots) = 0$, the identity element of $(G,\circ)$. Moreover,

$$\tau(g)\lambda(g')\tau(g)^{-1} = \lambda(g'+gg'),$$

so the image $\tau(G,\circ) = T$ is a regular subgroup of $\mathrm{Hol}(G)$.

This process is reversible: given a regular 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 $\tau(g)(x) = g\circ x$.

On $\circ$. For G elementary abelian, that is, $G\cong(\mathbb{F}_p^n,+)$, then $(G,\circ)$ is isomorphic to the group of principal units $1+A$ of the $\mathbb{F}_p$-algebra with identity

$$A_1 = \mathbb{F}_p 1 \oplus A.$$

The map is $f : A\to 1+A$ by $f(a) = 1+a$. Then

$$f(a\circ b) = 1+a\circ b = 1+a+b+ab = (1+a)(1+b).$$

Hence

$$\begin{aligned}1+a_1\circ a_2\circ\ldots\circ a_n &= f(a_1\circ a_2\circ\ldots\circ a)n)\\ &= f(a_1)f(a_2)\cdots f(a_n) = (1+a_1)(1+a_2)\cdots(1+a_n).\end{aligned}$$

In particular, if we define

$$a^{\circ n} = a\circ a\circ\ldots\circ a (n \text{ factors })$$

then we have what I'll call

Lemma 3 (Caranti's Lemma).

$$a^{\circ p} = \binom{p}{1}a + \binom{p}{2}a^2 + \ldots + \binom{p}{p-1}a^{p-1} + a^p.$$

Applications of nilpotent algebra structures, I. The third correspondence has turned out to be useful in several ways.

I. It yielded a new proof of an improved version of Featherstonhaugh's Theorem:

Let G be a finite abelian p-group of p-rank m. If $p > m+1$ then every regular abelian subgroup N of $Hol(G)$ is isomorphic to G.

For G elementary abelian, the theorem is:

Theorem 4. *Let G be an elementary abelian p-group of order p^n, and let T be a regular subgroup of* $\mathrm{Hol}(G)$*. If $p > n$, then $T \cong G$.*

The idea is if $A = (G, +, \cdot)$ is a (commutative, associative) nilpotent ring structure on $(G, +) \cong (\mathbb{F}_p^n, +)$, then $a^{n+1} = 0$ for all a in A. By Caranti's Lemma, $a^{\circ p} = a^p$. Since $a^{n+1} = 0$ and $n+1 \leq p$, $a^p = 0$, and so $(G, \circ)$ has exponent p, hence is elementary abelian of order p^n.

More generally, Caranti's proof of the main theorem of [FCC12] I believe can be modified to give

Proposition 5. *Let $p > 3$, prime, and $G = (G, +)$ be a finite abelian p-group of order p^n. Let $A = (G, +, \cdot)$ be a nilpotent ring structure on G and suppose $A^p = 0$. Then the regular subgroup $N = (G, \circ)$ of* $\mathrm{Hol}(G)$ *is isomorphic to $(G, +)$.*

Applications of nilpotent algebra structures, II. As I described in Omaha two years ago, (see [Ch15]) it is possible to get a lower bound on the number of isomorphism types of nilpotent algebra structures A on $G = (\mathbb{F}_p^n, +)$ with $A^3 = 0$. With the aid of an upper bound on isomorphism types of nilpotent algebras of dimension n of 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 $n \to \infty$.

The idea is to show that the number of isomorphism types of nilpotent algebras for large n is p to an exponent which is a function of order $2/27n^3$. Each isomorphism type corresponds to between 1 and

$|\mathrm{GL}_n(\mathbb{F}_p)| \sim p^{n^2}$ Hopf Galois structures, which asymptotically is irrelevant.

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.

Applications of nilpotent algebra structures, III. As I showed last year in Exeter (see [Ch16a]), if L/K is a Galois extension with elementary abelian Galois group G of order p^n and A is a nilpotent algebra structure on $G, +)$ with $A^3 = 0$, then the corresponding regular subgroup T of $\mathrm{Hol}(G)$ both normalizes and is normalized by $\lambda(G)$. Because of the latter, T yields a Hopf Galois structure on L/K directly, without translating from the holomorph to the permutation group.

Here's how it works.

The K-Hopf algebra H so that $H = LT^G$ consists of

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

which acts on a in L by

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

for a, b in L. Thus the multiplication in A is used to describe the Hopf algebra H and its action on L.

Since every Hopf Galois structure on a Galois extension of order p^2 corresponds to a nilpotent algebra A with $A^3 = 0$, this applies to all L/K Galois with Γ of order p^2 relatively easily, as was in fact observed in [By02].

It also applies to Hopf Galois structures arising from four of the five isomorphism types of nilpotent algebras A when $n = 3$, and for eight of the eleven isomorphism types of nilpotent algebras when $n = 4$.

Applications of nilpotent algebra structures, IV. The most recent and potentially the most interesting application of nilpotent algebras relates to the sub-Hopf algebra structure of Hopf algebras that arise from nilpotent algebras. This is from [Ch16b].

A bit of background: the Fundamental Theorem of Galois Theory (FTGT) of Chase and Sweedler [CS69] states that if L/K is a H-Hopf Galois extension of fields for H a K-Hopf algebra H, then there is an injection $\mathcal{F}$ from the set of K-sub-Hopf algebras of H to the set of intermediate fields $K \subseteq E \subseteq L$ given by sending a K-subHopf algebra J to $\mathcal{F}(J) = L^J$. The *strong form* of the FTGT holds if the injection is also a surjection.

Cases where the strong form of FTGT fails. For a classical Galois extension of fields with Galois group Γ, the FTGT holds in its strong form. But it is known from [GP87] that if L/K is a (classical) Galois extension with non-abelian Galois group Γ, then there is a Hopf Galois structure on L/K, the one corresponding to the regular subgroup $\lambda(\Gamma)$ of $\mathrm{Perm}(\Gamma)$ so that the Galois correspondence map $\mathcal{F}$ maps onto the subfields E of L that are normal over K. So if Γ is not a Hamiltonian group, then L/K has a Hopf Galois structure for which the strong form of the FTGT does not hold.

In particular, the strong form fails extremely for the unique [By04] non-classical Hopf Galois structure on L/K (corresponding to $\lambda(\Gamma)$) when Γ is a non-abelian simple group.

An abelian example. Perhaps the only wholly abelian example of failure in the literature is in [CRV15], 3.1: let $\Gamma \cong C_2 \times C_2$, then L/K has a Hopf Galois structure by H, a K-Hopf algebra of type C_4. Then by classical Galois theory, there are three intermediate subfields between K and L, but C_4 has only one intermediate subgroup, so H can have at most one intermediate K-subHopf algebra. Hence the strong form of the FTGT cannot hold for that Hopf Galois structure.

From [CRV16]. To approach this question we start with a result of Crespo, Rio and Vela ([CRV16], Proposition 2.2),:

Proposition 6 (CRV16). *If L/K is Galois with Galois group Γ and is H-Hopf Galois where $L \otimes_K HcongLN$ with N a regular subgroup of* $\mathrm{Perm}(\Gamma)$ *normalized by $\lambda(\Gamma)$, then the K-subHopf algebras of H correspond to the subgroups of N that are normalized by $\lambda(\Gamma)$.*

Applying nilpotent algebras to the FTGT.

Theorem 7. *Let G be a finite abelian p-group, written additively. Suppose the nilpotent algebra $A = (G, +, \cdot)$ yields the 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 where H corresponds to $\alpha(G)$. Then the lattice (under inclusion) of $\lambda(\Gamma)$-invariant subgroups of $\alpha(G)$, and hence the lattice of K-sub-Hopf algebras of H, is isomorphic to the lattice of ideals of A.*

Subgroups of $\alpha(G)$ correspond to subgroups of G.

Proof. First, $\alpha : G \to Perm(\Gamma)$ is an injective homomorphism from $(G, +)$ to $\mathrm{Perm}(\Gamma)$. So additive subgroups of G correspond to additive subgroups of $\alpha(G) \subset \mathrm{Perm}(G)$.

Concerning ideals and λ-invariance. Suppose the image $\alpha(G)$ of α is normalized by $\lambda(\Gamma)$. Then for all γ in Γ, g in G, there is some h in G so that

$$\lambda(\gamma)\alpha(g)\lambda(\gamma)^{-1} = \alpha(h).$$

By Proposition 1, this equation holds iff

$$\beta(\gamma)\lambda_G(g) = \lambda_G(h)\beta(\gamma).$$

Recalling that $A = (G, +, \cdot) = (G, \circ)$, factor $\beta = \tau\xi$ where $\xi : \Gamma \to A = (G, \circ)$ is an isomorphism and $\tau : A = (G, \circ) \to Hol(G)$ sends k in G to $\tau(k)$ where $\tau(k)(y) = k \circ y$ for y in G. Let $\xi(\gamma) = k$ in A. Then the last equation is

$$\tau(k)\lambda_G(g) = \lambda_G(h)\tau(k),$$

and applying this to x in G gives

$$\tau(k)(g + x) = h + \tau(k)(x).$$

Since $\tau(k)(x) = k \circ x$, we have

$$k \circ (g + x) = h + k \circ x.$$

Viewing this equation in A, where $a \circ b = a + b + a \cdot b$, we have

$$k + (g + x) + k \cdot g + k \cdot x = h + k + x + k \cdot x.$$

This last equation reduces to

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

Invariant subgroups of $\alpha(G)$ correspond to ideals of A. Now suppose J is an ideal of A and g is in J. Then $k \cdot g$ is in J, so h is in J, and so $\lambda(\gamma)$ conjugates $\alpha(g)$ in $\alpha(J)$ to an element of $\alpha(J)$. So $\alpha(J)$ is normalized by $\lambda(\Gamma)$ in $\mathrm{Perm}(\Gamma)$.

Conversely, suppose J is an additive subgroup of $(G, +, \cdot) = A$ and $\alpha(J)$ is normalized by $\lambda(\Gamma)$. Then for all γ in G, g in J,

$$\lambda(\gamma)\alpha(g)\lambda(\gamma)^{-1} = \alpha(h)$$

and $\alpha(h)$ is in $\alpha(J)$. So h is in J. Then by Proposition 1 as above, for all $k = \xi(\gamma)$ in G, and g in J, $h = g + k \cdot g$ is in J. Now J is an additive subgroup of A, so $k \cdot g$ is in J for all k in G, g in J. Thus J is an ideal of A. $\square$

Failure of strongness.

Theorem 8. *Let L/K be a Galois extension of fields with Galois group Γ an elementary abelian p-group of order p^n. Let L/K have a Hopf Galois structure by an abelian Hopf algebra H of type G where G is an elementary abelian p-group. Let A be the nilpotent ring structure yielding the regular subgroup $T \cong (G, \circ) \subset \mathrm{Hol}(G)$ corresponding to H, where $(G, \circ) \cong \Gamma$. Then the H-Hopf Galois structure on L/K satisfies the strong form of the FTGT if and only if H is the classical Galois structure by $K\Gamma$ on L/K.*

Proof. If $A^2 = 0$, then $(G, \circ) = (G, +)$, so the regular subgroup T acts on G by $\tau(g)(h) = g \circ h = g + h$, hence $T = \lambda(G)$. Since G is abelian, the corresponding Hopf Galois structure on L/K is the classical structure by the K-Hopf algebra $K[\Gamma]$. So the Galois correspondence holds in its strong form.

The converse. For the converse, view $(G, +)$ as an n-dimensional $\mathbb{F}_p$-vector space. Suppose $A^2 \neq 0$. Then for some a, b in A, $ab \neq 0$. Then the subspace $\mathbb{F}_p a$ does not contain ab. For if $ab = ra$ for $r \neq 0$ in $\mathbb{F}_p$, then $a = sba$ for $s \neq 0$ in $\mathbb{F}_p$. Then

$$a = (sb)a = (sb)^2 a = \ldots = (sb)^k a$$

for all $k \geq 1$. Since A is nilpotent, $(sb)^k = 0$ for some k. Thus the subspace $\mathbb{F}_p a$ is not an ideal of A.

Mopping up. The subgroup $\alpha(\mathbb{F}_p a)$ of $\alpha(G)$ is then not normalized by $\lambda(\Gamma)$. But $\Gamma \cong G$, so there are bijections between subgroups of $\alpha(G)$, subgroups of G, subgroups of Γ and (by classical Galois theory) subfields of L containing K. If some subgroup of $\alpha(G)$ is not normalized by $\lambda(\Gamma)$, then the number of K- subHopf algebras of $H = L[\alpha(G)]^G$ is strictly smaller than the number of subfields between K and L. So the Galois correspondence for the H-Hopf Galois structure on L/K does not hold in its strong form. $\square$

There are many examples. If G is an elementary abelian p-group of order p^n and $T \cong (G, \circ)$ is a regular subgroup of $\mathrm{Hol}(G)$ corresponding to a nilpotent ring structure $A = (G, +, \cdot)$ with $A^p = 0$, then $(G, \circ)$ is an abelian group of exponent p by Caranti's Lemma, noted earlier, so is isomorphic to G. Hence every isomorphism type of nilpotent $\mathbb{F}_p$-algebra A of dimension n with $A^p = 0$ yields a Hopf Galois structure on a Galois extension L/K with Galois group $\Gamma \cong G$ for which the strong form of the FTGT fails. By [Ch15], there are many examples for large n.

The cyclic case.

Proposition 9. *Let L/K be a Galois extension of fields with Galois group Γ cyclic of order p^n, p odd. Let the K-Hopf algebra H give a Hopf Galois structure on L/K. Then H has type G where $G \cong \Gamma$, and the Galois correspondence for that Hopf Galois structure holds in its strong form.*

One can show that the commutative nilpotent algebra structures on $(\mathbb{Z}/p^n\mathbb{Z}, +)$ have the form A_d for d modulo p^{n-1}, where for r, s in $(\mathbb{Z}/p^n\mathbb{Z}, +)$, the multiplication is

$$r \cdot s = rspd.$$

It is then easy to check that the ideals of A_d are the principal ideals generated by p^r, for $r = 0, \ldots, n$. Since there are only $n+1$ intermediate fields E with $K \subseteq E \subseteq L$, the theorem above implies that for every Hopf Galois structure on L/K, the Galois correspondence holds in its strong form.

Egregious failure of the strong form. Return to the elementary abelian case with $\Gamma \cong G = (\mathbb{F}_p^n, +)$.

Let A be the primitive n-dimensional nilpotent $\mathbb{F}_p$-algebra generated by z with $z^{n+1} = 0$. Then $(A, +) \cong (\mathbb{F}_p^n, +)$ and so the multiplication on A yields a nilpotent $\mathbb{F}_p$-algebra structure on $(G, +) = (\mathbb{F}_p^n, +)$. Let $\Gamma \cong (\mathbb{F}_p^n, \circ)$ where the operation $\circ$ is defined using the multiplication on A by $a \circ b = a + b + a \cdot b$.

Theorem 10. *Let G be an elementary abelian p-group of order p^n. Let A be a primitive $\mathbb{F}_p$-algebra structure A on G, and let $(G, \circ)$ be the corresponding group structure on $\mathbb{F}_p^n$. Suppose L/K is a Galois extension of fields with Galois group $\Gamma \cong (G, \circ)$. Then the primitive nilpotent $\mathbb{F}_p$-algebra A corresponds to an H-Hopf Galois structure on L/K for some K-Hopf algebra H, where the K-subHopf algebras of H form a descending chain*

$$H = H_1 \supset H_2 \supset \ldots \supset H_n \supset K.$$

Hence the Galois correspondence $\mathcal{F}$ for H maps onto exactly $n+1$ fields F with $K \subseteq F \subseteq L$.

Given Theorem 7, we just need to show that ideals of A are $J_i = \langle z^i \rangle$ for $i = 1, \ldots, n$, which is pretty routine.

Since the correspondence between ideals of A and $\lambda(\Gamma)$ invariant subgroups of $\alpha(G)$ is lattice-preserving, we have a single filtration

$$\alpha(G) = \alpha(J_1) \supset \alpha(J_2) \supset \ldots \supset \alpha(J_n) \supset 0.$$

of $\lambda(G)$-invariant subgroups of $\alpha(G)$. If H is the corresponding K-Hopf algebra making L/K into a Hopf Galois extension, then H has a unique filtration of K-sub-Hopf algebras,

$$H = H_1 \supset H_2 \supset \ldots \supset H_n \supset K.$$

How egregious? For A a primitive nilpotent $\mathbb{F}_p$-algebra with $A^{n+1} = 0$, the corresponding group $(G, \circ)$ is isomorphic (by $a \mapsto 1 + a$) to the group of principal units of the truncated polynomial ring $\mathbb{F}_p[x]/(x^{n+1}\mathbb{F}_p[x]$. For its structure, see [Ch07]. In particular $(G, \circ)$, hence Γ, is an elementary abelian p-group if and only if $p > n$.

Thus in the last theorem, when $p > n$, then L/K is classically Galois with Galois group $\Gamma \cong (\mathbb{F}_p^n, +)$. So the number of subgroups of Γ, and hence the the number of subfields E with $K \subseteq E \subseteq L$, is equal to the number of subspaces of $\mathbb{F}_p^n$, namely

$$\sum_{r=1}^{n} \frac{(p^n - 1)(p^n - p)\cdots(p^n - p^{r-1})}{(p^r - 1)(p^r - p)\cdots(p^r - p^{r-1})} \sim np^n$$

for n large. So the Galois correspondence map $\mathcal{F}$ is extremely far from being surjective for a Hopf Galois structure corresponding to a nilpotent algebra structure A with $\dim(A/A^2) = 1$.

$n = 2$**.** One collection of examples in the literature are the non-trivial Hopf Galois structures on a Galois extension L/K of degree p^2 with Galois group $G \cong (\mathbb{F}_p^2, +)$. All of them correspond to nilpotent $\mathbb{F}_p$-algebras A with $\dim(A/A^2) = 1, A^3 = 0$. If x_1, x_2 is a $\mathbb{F}_p$-basis of G and the multiplication on $A = (G, +)$ is by $x_1^2 = dx_2$ with $d \neq 0$ and $x_2 x_i = 0$ for $i = 1, 2$, then the corresponding K-Hopf algebra has the form $H_{T,d}$, in the notation of [By02], and have type G. So in retrospect, all of those non-classical Hopf Galois structures were abelian examples of the failure of the strong form of the FTGT.

References

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

[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.

[CDVS06] A. Caranti, F. Dalla Volta, M. Sala, Abelian regular subgroups of the affine group and radical rings. Publ. Math. Debrecen 69 (2006), 297–308.

[CS69] S. U. Chase, M. E. Sweedler, Hopf Algebras and Galois Theory, Springer LNM 97 (1969).

[Ch89] L. N. Childs, On the Hopf Galois theory for separable field extensions, Comm. Algebra 17 (1989), 809–825.

[Ch07] L. N. Childs, Some Hopf Galois structures arising from elementary abelian p-groups, Proc. Amer. Math. Soc. 135 (2007), 3453–3460.

[Ch11] L. N. Childs, Hopf Galois structures on Kummer extensions of prime power degree, New York J. Math. 17 (2011). 5174.

[Ch15] L. N. Childs, On Abelian Hopf Galois structures and finite commutative nilpotent rings, New York J. Math., 21 (2015), 205–229.

[Ch16a] L. N. Childs, Obtaining abelian Hopf Galois structures from finite commutative nilpotent rings, arxiv: 1604.05269

[Ch16b] L. N. Childs, On the Galois correspondence for Hopf Galois extensions, arxiv:1604.06066

[CRV15] T. Crespo, A. Rio, M. Vela, From Galois to Hopf Galois: theory and practice, Contemp. Math. 649 (2015), 29–46.

[CRV16] T. Crespo, A. Rio, M. Vela, On the Galois correspondence theorem in separable Hopf Galois theory, Pub. Mat. Debrecen 60 (2016), 221–234.

[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.

[Ha59] M. Hall, The Theory of Groups, Macmillan, New York, 1959.

[Ko98] T.Kohl, Classification of the Hopf Galois structures on prime power radical extensions, J. Algebra 207 (1998), 525–546.

University at Albany