HOPF GALOIS STRUCTURES FOR TOTALLY RAMIFIED p-ELEMENTARY ABELIAN GALOIS EXTENSIONS

LINDSAY N. CHILDS

This is a somewhat edited version of a short talk given at the 2016 Omaha workshop on Hopf Galois Structures and Galois Module Theory, May 26, 2016.

Egregious failure of the strong form of FTGT. Let L/K be a field extension with Galois group isomorphic to $\Gamma \cong G = (\mathbb{F}_p^n, +)$. Assume $p > n$.

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 $a \circ b = a + b + a \cdot b$. If $p > n$ then $(\mathbb{F}_p^n, \circ) \cong (\mathbb{F}_p^n, +)$.

In my other talk I described how a nilpotent $\mathbb{F}_p$-algebra structure A on $(G, +)$ yields Hopf Galois structures on L/K by a K-Hopf algebra H associated to A, and related the surjectivity of the Galois correspondence from K-subHopf algebras of H to intermeditate fields between K and L to the ideal structure of A (using the main theorem from [Ch16b]). That led to the following set of examples:

Theorem 1. *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 single 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 $K \subseteq F \subseteq L$.

So the Hopf Galois structures arising from a primitive nilpotent algebra A seem to have a particularly rigid set of intermediate fields.

Date: June 10, 2016.

The question I wondered about is, are these Hopf Galois structures interesting for local Galois module theory? The bottom line is that I don't know.

In the rest of these notes I start looking at what the corresponding regular subgroups of $\mathrm{Perm}(\Gamma)$ look like for a primitive nilpotent algebra. In an Appendix, I look briefly at the ideal structure of the four other isomorphism classes of nilpotent algebras over $\mathbb{F}_p$ of dimension 3.

Let $G \cong (\mathbb{F}_p^n, +)$, let A be a nilpotent $\mathbb{F}_p$-algebra structure on $(G, +)$. Let $(G, \circ)$ be the corresponding group structure, where

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

Let T be the corresponding regular subgroup of $\mathrm{Hol}(G, +)$. Then

$$T = \{\tau(g) : g \in G\} \subset \mathrm{Perm}(G)$$

where $\tau(g)(x) = g \circ x$, hence $\tau(g)\tau(h) = \tau(g \circ h)$ in T. Thus

$$\tau : (G, \circ) \to T$$

is an isomorphism from $(G, \circ)$ into $\mathrm{Perm}(G)$.

Let L/K be a Galois extension of fields with abelian Galois group Γ of order p^n. Let $b : \Gamma \to (G, \circ)$ be an isomorphism of groups. Then the map

$$\beta = \tau b : \Gamma \to T$$

is a regular embedding of Γ into $\mathrm{Hol}(G)$.

The corresponding regular embedding $\alpha : G \to \mathrm{Perm}(\Gamma)$ is defined by

$$\alpha(g) = b^{-1}(\lambda(g))b :$$

for x in G, $\alpha(g)(x) = b^{-1}(\lambda(g)b(x))$.

Then $\lambda(\Gamma)$ normalizes $\alpha(G)$ in $\mathrm{Perm}(G)$: in fact, for $b(\gamma) = g$ in G,

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

So $\alpha(G)$ yields by descent the K-Hopf algebra $H = L[\alpha(G)]^\Gamma$ corresponding to A and the isomorphism $b : \Gamma \to (G, \circ)$, and H acts on L as follows: if

$$h = \sum_{g \in G} s_g \alpha(g)$$

then for t in L,

$$h(t) = \sum_{\gamma \in \Gamma} s_{-b(\gamma)} \gamma(t).$$

n=2. Let L/K be a Galois extension of fields with Galois group Γ an elementary abelian p-group of order p^2, and let G also be an elementary abelian p-group of order p^2. Let x_1, x_2 be a basis of $G \cong (\mathbb{F}_p^2, +)$ and define a nilpotent ring structure on G by setting $x_1^2 = dx_2$ and $x_2 \cdot x_i = 0$ for $i = 1, 2$. This defines the circle multiplication on G by

$$y \circ w = y + w + y \cdot w$$

for all y, w in $(G, +)$. We define an isomorphism $b : \Gamma \to (G, \circ)$ by picking a basis u_1, u_2 for Γ and setting $b(u_1) = x_1, b(u_2) = x_2$. Then

$$b(u_1^{r_1} u_2^{r_2}) = x_1^{\circ r_1} \circ x_2^{\circ r_2} = r_1 x_1 + (\binom{r_2}{2} d + r_2) x_2.$$

or in terms of components relative to the two bases for Γ and G,

$$b(\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} (r_1 \\ r_2 + \binom{r_1}{2} d \end{pmatrix}.$$

Then

$$b^{-1} \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} = \begin{pmatrix} s_1 \\ s_2 - \binom{s_1}{2} d \end{pmatrix}.$$

We then define $\alpha : (G, +) \to \mathrm{Perm}(G)$ by

$$\begin{aligned} \alpha(\overline{r})(\overline{t}) &= b^{-1}(\lambda(\overline{r})(b(\overline{t}))) \\ &= b^{-1} \begin{pmatrix} r_1 + t_1 \\ r_2 + t_2 + \binom{t_1}{2} d \end{pmatrix} = \begin{pmatrix} r_1 + t_1 \\ r_2 + t_2 + \binom{t_1}{2} d - \binom{r_1 + t_1}{2} d \end{pmatrix} \end{aligned}$$

In particular,

$$\alpha \begin{pmatrix} 0 \\ 1 \end{pmatrix} (\overline{t}) = \begin{pmatrix} t_1 \\ 1 + t_2 \end{pmatrix}$$

$$\alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} (\overline{t}) = \begin{pmatrix} t_1 + 1 \\ t_2 - t_1 d \end{pmatrix}.$$

Thus the unique K-subHopf algebra of H corresponds to the subgroup $\alpha(\langle x_2 \rangle)$, which acts on G like $\langle \lambda(u_2) \rangle$.

Comparing with [By02]. Byott obtains $p^2 - 1$ non-classical Hopf Galois structures on a Galois extension of order p^2 with Galois group G. They have the form $H_{T,d}$ where T is a subgroup of Γ of order p and d is in $\mathbb{F}_p$. The regular subgroup of $\mathrm{Perm}(\Gamma)$ corresponding to $H_{T,d}$ is $\langle \eta, \rho \rangle$. We obtain $H_{T,d}$ by our construction by letting $T = \langle u_2 \rangle$. Then the permutations $\alpha(x_1) = \eta^{-1}$ and $\alpha(x_2) = \rho^{-1}$.

So for $n = 2$ a nilpotent multiplication A on the Galois group G with $\dim(A/A^2) = 1$ yields all of the non-trivial Hopf Galois structures on L/K.

Each Hopf Galois structure defined by a primitive nilpotent algebra A is by a K-Hopf algebra H with a unique K-subHopf algebra of order p, namely $L[\alpha(x_2)]^G \cong K[\lambda(u_2)]$.

Suppose L/K is a totally ramified Galois extension of local fields with Galois group G elementary abelian of order p^2, and has two ramification breaks:

$$G = G_1 > G_2 > (1).$$

Byott showed that if L/K is H-Hopf Galois for a non-classical Hopf algebra $H_{T,d}$, and the associated order in $H_{T,d}$ of $\mathfrak{O}_L$ is a Hopf order, then the unique K-subHopf algebra H_2 of $H_{T,d}$ acts on L like the group ring of the ramification group $K[G_2]$. The fixed field of the unique subHopf algebra of $H_{T,d}$ is the fixed field of the ramification group G_2.

That observation invites a look at what these Hopf Galois structures look like for $n > 2$.

$n = 3$. For $n = 3$ define a multiplication on $(G, +) = \mathbb{F}_p x_1 + \mathbb{F}_p x_2 + \mathbb{F}_p x_3$ by

$$x_1^2 = d_2x_2 + d_3x_3, \quad x_1x_2 = d'x_3$$

and all other products of x_1, x_2, x_3 are 0. Then for $m > 1$,

$$x_1^{\circ m} = mx_1 + \binom{m}{2}(d_2x_2 + d_3x_3) + \binom{m}{3}d'd_3x_3.$$

Picking a basis u_1, u_2, u_3 of Γ and letting $b : \Gamma \to (G, \circ)$ by $b(u_i) = x_i$, we get

$$b(\overline{r}) = \begin{pmatrix} r_1 \\ r_2 + \binom{r_1}{2}d_2 \\ r_3 + r_1r_2d' + \binom{r_1}{2}d_3 + \binom{r_1}{3}d_2d' \end{pmatrix} = \begin{pmatrix} r_1 \\ r_2 + p_2(r_1) \\ r_3 + p_3(r_1, r_2) \end{pmatrix}$$

for some polynomials $p_2(x_1), p_3(x_1, x_2)$. Then b^{-1} has the same form.

The special case where the basis of A is z, z^2, z^3 ($d_2 = d' = 1, d_3 = 0$) is slightly nicer. If we write

$$\overline{r} = r_1u_1 + r_2u_2 + r_3u_2 = \begin{pmatrix} r_1 \\ r_2 \\ r_3 \end{pmatrix}, \overline{s} = s_1x_1 + s_2x_2 + s_3x_3 = \begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix},$$

and $b : \Gamma \to (G, \circ)$ is a homomorphism with $b(u_i) = x_i$, then

$$\overline{s} = b(\overline{r}) = \begin{pmatrix} r_1 \\ r_2 + \binom{r_1}{2} \\ r_3 + r_1r_2 + \binom{r_1}{3} \end{pmatrix}.$$

Then b^{-1} satisfies

$$\overline{r} = b^{-1}(\overline{s}) = \begin{pmatrix} s_1 \\ s_2 - \binom{s_1}{2} \\ s_3 - s_1 s_2 + s_1\binom{s_1}{2} - \binom{s_1}{3} \end{pmatrix}.$$

To obtain a regular subgroup of $\mathrm{Perm}(\Gamma)$ from β, we define the embedding $\alpha : G \to \mathrm{Perm}(\Gamma)$ by

$$\alpha(\overline{r}) = b^{-1}\lambda(\overline{r})b : G \to \mathrm{Perm}(\Gamma).$$

Thus

$$\begin{aligned} \alpha(\overline{r})(\overline{t}) &= b^{-1}\lambda(\overline{r})b(\overline{t}) \\ &= b^{-1}\lambda(\overline{r}) \begin{pmatrix} t_1 \\ t_2 + \binom{t_1}{2} \\ t_3 + t_1 t_2 + \binom{t_1}{3} \end{pmatrix} \\ &= \begin{pmatrix} r_1 + t_1 \\ r_2 + t_2 - \frac{r_1^2}{2} - r_1 t_1 + \frac{r_1}{2} \\ f \end{pmatrix} \end{aligned}$$

where

$$\begin{aligned} f &= r_3 + t_3 - r_1 r_2 - r_1 t_2 - r_2 t_1 \\ &\quad - \frac{r_1}{3} + \frac{r_1 t_1}{2} + \frac{r_1^3}{3} + r_1^2 t_1 + \frac{r_1 t_1^2}{2}. \end{aligned}$$

Then α has a "triangular" form. So

$\alpha(x_3)$ acts on $\Gamma_3 = K\langle u_3\rangle$ like $\lambda(u_3)$;

modulo Γ_3, $\alpha(x_2)$ acts on Γ_2 like $\lambda(u_2)$, and

modulo Γ_2, $\alpha(x_1)$ acts on Γ_1 like $\lambda(u_1)$.

Hardly surprising–the subquotient Hopf algebras of H of K-dimension p must be isomorphic to $K[C_p]$.

General n**.** Let $G = (\mathbb{F}_p^n, +)$ and define the primitive nilpotent $\mathbb{F}_p$-algebra structure $(A = (\mathbb{F}_p^n, +, \cdot)$ on G by picking a basis $(x_1, \ldots, x_n)$ for $\mathbb{F}_p^n$, let $z = x_1$ and let $x_k = z^k$ for $k \geq 1$, and $z^{n+1} = 0$. This is quite special, but a more general case should be derivable from this case by applying a unipotent change of basis to A.

We show that describing the corresponding regular subgroup $\alpha(G)$ of $\mathrm{Perm}(\Gamma)$ is computationally manageable.

The corresponding group structure $(A, \circ)$ is defined by

$$z^i \circ z^j = z^i + z^j + z^{i+j}.$$

Let $\mathbb{F}_p[x]$ be the polynomial ring, Then the map $y \mapsto 1+y$ defines an isomorphism from $(A, \circ)$ to the group $(1+x)\mathbb{F}_p[x]/x^{n+1}\mathbb{F}_p[x]$ of principal units of $\mathbb{F}_p[x]/x^{n+1}\mathbb{F}_p[x]$. For

$$a \circ b \mapsto 1 + a \circ b = 1 + a + b + a \cdot b = (1+a) \cdot (1+b).$$

So for all $a_1, \ldots a_n$ in $(A, \circ)$,

$$a_1 \circ a_2 \circ \ldots \circ a_m \mapsto (1+a_1) \cdot (1+a_2) \cdot \ldots \cdot (1+a_n).$$

Since $p > n$, $(G, \circ)$ is an elementary abelian p-group with p-basis $z, z^2, \ldots, z^n$ (by [Ch07]). So let $\Gamma = (\mathbb{F}_p^n, +)$ have basis $u_1, \ldots, u_n$ and define an isomorphism $b : \Gamma \to (\mathbb{F}_p, \circ)$ by $b(u_i) = z^i$ for $i = 1, \ldots, n$, and

$$\begin{aligned} b(\sum_i r_i u_i) &= (r_1 \circ z) \circ (r_2 \circ z^2) \circ \ldots \circ (r_n \circ z^n) \\ &= (1+z)^{r_1} \cdot (1+z^2)^{r_2} \cdot \ldots \cdot (1+z^n)^{r_n}. \end{aligned}$$

Define $\beta = \tau b : \Gamma \to T \subset \mathrm{Hol}(G)$. Then β is a regular embedding of Γ in $\mathrm{Hol}(G)$ and $\beta(\gamma)(0) = \tau(\xi(\gamma))(0) = b(\gamma)$.

To obtain the corresponding Hopf Galois structure on L/K, we construct the embedding $\alpha : G \to Perm(\Gamma)$ corresponding to β, by

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

So we need to describe b^{-1}. Since $z^{n+1} = 0$, there exist $s_1, \ldots, s_n$ in $\mathbb{F}_p$ so that

$$b(\sum_i r_i u_i) = (1+z)^{r_1} \cdot (1+z^2)^{r_2} \cdot \ldots \cdot (1+z^n)^{r_n} = \sum_{j=1}^{n} s_j z^j.$$

To find b^{-1}, that is, to find $r_1, \ldots, r_n$ in terms of $s_1, \ldots, s_n$ we can use the logarithm function

$$\log_z(1+w) = \sum_{i=1}^{n} (-1)^{i+1} \frac{w^i}{i}.$$

for w in $z\mathbb{F}_p[z]/z^{n+1}\mathbb{F}_p[z]$. For w_1, w_2 multiples of z,

$$\log_z((1+w_1)(1+w_2) = \log_z(1+w_1) + \log_z(1+w_2).$$

Applying $\log_z$ to the equation for $s_1, \ldots, s_n$:

$$(1+z)^{r_1}(1+z^2)^{r_2} \cdot \ldots \cdot (1+z^n)^{r_n} = s_1 z_1 + \ldots z_n z_n$$

yields

$$\sum_{i=1}^{n} \log_z((1+z^i)^{r_i}) = \log_z(s_1 z_1 + \ldots z_n z_n)$$

or

$$\sum_{i=1}^{n} r_i \sum_{k=1}^{n} \frac{(-1)^{k+1}}{k} z^{ik} = \sum_{j=1}^{n} \frac{(-1)^{i+1}}{i} (s_1 z + \ldots + s_n z^n)^i).$$

Modulo $z^2, z^3, \ldots$, one can see that $r_1 = s_1$ and there are polynomials $f_{i+1}(x_1, \ldots, x_n), g_{i+1}(x_1, \ldots, x_i)$ for $i = 1, 2, \ldots, n-1$ so that

$$r_{i+1} + f_{i+1}(r_1, \ldots, r_i) = s_{i+1} + g_{i+1}(s_1, \ldots, s_i).$$

Hence for $i = i, \ldots, n$,

$$s_i = r_i + (\text{ polynomial function of } r_1, \ldots, r_{i-1})$$
$$r_i = s_i + (\text{ polynomial function of } s_1, \ldots, s_{i-1}).$$

For a nilpotent algebra structure A on $(\mathbb{F}_p^n, +)$ with $\dim(A/A^2) = 1$, there is a unique chain

$$\alpha(G) = N_1 > N_2 > \ldots > N_n > (1)$$

of subgroups of $\alpha(A)$, and a corresponding chain

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

of K-subHopf algebras of the Hopf algebra H corresponding to A, hence a corresponding chain of invariant subfields of L. This chain of subfields in turn corresponds to a unique chain

$$\Gamma = \Gamma_1 > \Gamma_2 > \ldots > \Gamma_n > (1)$$

of subgroups of the Galois group Γ of L/K.

Because of the form of b and b^{-1}, we see that N_i acts on Γ_i/Γ_{i+1} like $\lambda(\Gamma_i)$ for all i, and so $H_i//H_{i+1} \cong K[\Gamma_i/\Gamma_{i+1}]$.

Griff asked for "crazy ideas". Here is mine, speculating from the case $n = 2$:

Crazy idea: Let L/K be a totally ramified Galois extension of local fields of residue characteristic p with Galois group $\Gamma = C_p^n$ with $p > n$, Suppose L/K has a non-classical H-Hopf Galois extension of type $G \cong \Gamma$ corresponding to a primitive nilpotent algebra structure on G. Suppose $\mathfrak{O}_L$ is an $\mathfrak{A}_H$- Hopf Galois extension of $\mathfrak{O}_K$ for $\mathfrak{A}_H$ the associated order in H. (So $\mathfrak{A}_H$ is Hopf.) If

$$\Gamma = \Gamma_1 > \Gamma_2 > \ldots > \Gamma_n > (1)$$

is the ramification filtration of Γ, with fixed fields

$$K = K_1 \subset K_2 \subset \ldots \subset K_n \subset L,$$

then the K-Hopf algebra H must correspond to a primitive nilpotent algebra structure A on G, and the Hopf subalgebras of H arising from the ideals of A must have the same chain of fixed fields as the ramification filtration of Γ.

This is false in general, even for $n = 2$. But it would be interesting to use the p^2 classification of Byott to see how the parameters i, j in that classification relate to the possible ideal structure of the nilpotent algebra A associated to a Hopf Galois structure H on L/K. I haven't had a chance to do this yet.

Appendix: The ideal structure of nilpotent algebras of dimension $n = 3$

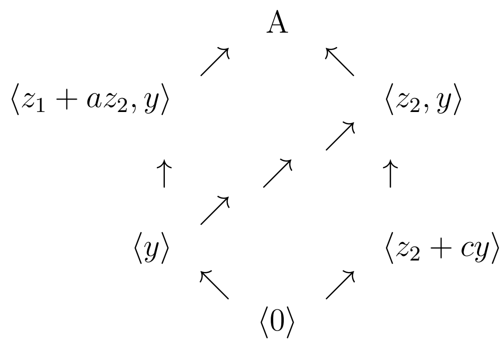
For $n = 3$ we can pick representatives of the five isomorphism types of nilpotent algebra structures A on $G = (\mathbb{F}_p^3, +)$ and look at the corresponding ideal structures. At the very least these examples describe the possible K-subHopf algebras of the Hopf Galois structures corresponding to the different A.

$A^2 = 0$. When $A^2 = 0$, the multiplicative structure on G is trivial. In that case, the corresponding Hopf Galois structure on L/K is the classical structure corresponding to the regular subgroup $\lambda(G) = \rho(G)$ of $\mathrm{Perm}(G)$. Every additive subgroup of A is an ideal, and every subgroup N of $\lambda(G)$ is $\lambda(G)$-invariant, hence yields a subHopf algebra of KG, namely the group ring KN.

$\dim(A/A^2) = 1$. This is the case where A is primitive. We described that situation above.

$\dim(A^2) = 1$. In this case $A^3 = 0$ and we described the isomorphism types of nilpotent algebra structures A on $(G, +)$ in Section 6 of [Ch16a]. By choosing a basis appropriately, we can assume that A has a basis (z_1, z_2, y) where $z_1^2 = y, z_2^2 = sy$, $z_1 z_2 = 0$ and $ya = 0$ for all a in A. We may further assume that $s = 0, 1$ or a non-square s'. The cases $s = 1, s = s'$ are identical for the ideal structure.

$s = 0$. Here is the lattice of ideals of A:



An arrow means inclusion. The parameters a, c runs through all elements of $\mathbb{F}_p$ (so $\langle z_2 + c\rangle$ is one of p ideals in that position, one for each c in $\mathbb{F}_p$, and $\langle z_1 + az_2, y\rangle$ is one of p ideals in that position).

In terms of the surjectivity of the FTGT, here is a table counting the number of subspaces and the number of ideals of a given dimenision over $\mathbb{F}_p$:

dimension	# subspaces	# ideals	# non-ideal subspaces
0	1	1	0
1	p^2+p+1	$p+1$	p^2
2	p^2+p+1	$p+1$	p^2
3	1	1	0

$s = 1$ **or** $= s'$**.** Here is the lattice of ideals of A:

$$\begin{array}{c} A \\ \uparrow \\ \langle y, az_1 + bz_2\rangle \\ \uparrow \\ \langle y\rangle \\ \uparrow \\ \langle 0\rangle \end{array}$$

Here a, b runs through all elements of $\mathbb{F}_p$, so $\langle y, az_1 + bz_2\rangle$ stands for p^2 ideals in that position.

In terms of the surjectivity of the FTGT, here is a table counting the number of subspaces and the number of ideals of a given dimenision over $\mathbb{F}_p$:

dimension	# subspaces	# ideals	# non-ideal subspaces
0	1	1	0
1	p^2+p+1	1	p^2+p
2	p^2+p+1	$p+1$	p^2
3	1	1	0

Suppose L/K is totally ramified with Galois group $G \cong (F_p^3, +)$ and is H-Hopf Galois for some non-classical K-Hopf algebra H corresponding to a nilpotent algebra structure A on G. The work in [By02] suggests that for some sets of break numbers, if the associated order $\mathfrak{A}$ of the valuation ring S in H is a Hopf order so that S is $\mathfrak{A}$-Hopf Galois over R, then there are restrictions on the break numbers of L/K and on the sub-Hopf algebras of H, enough so that in some cases the restrictions define limitations on the lattice of subHopf algebras of H, which correspond to limitations on the ideals of A.

In particular, by analogy with the case $n = 2$, there may be cases involving three distinct break numbers where the only Hopf Galois structures on L/K of interest will correspond to the primitive nilpotent algebra structure looked at earlier in these notes, where the subfields of L fixed by subHopf algebras of H are the subfields fixed by the ramification subgroups of G.

Obviously this line of investigation is just beginning.

References

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

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

[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