New York Journal of Mathematics

New York J. Math. **25** (2019) 1421–1437.

Abelian Hopf Galois structures from almost trivial commutative nilpotent algebras

Lindsay N. Childs

Abstract. Let L/K be a Galois extension of fields with Galois group G an elementary abelian p-group of rank n for p an odd prime. It is known that nilpotent $\mathbb{F}_p$-algebra structures A on G yield regular subgroups of the holomorph $\mathrm{Hol}(G)$, hence Hopf Galois structures on L/K. In this paper we illustrate the richness of Hopf Galois structures on L/K by examining the case where A is abelian of $\mathbb{F}_p$-dimension n where $\dim(A^2) = 1$. We determine the number of Hopf Galois structures that arise in these cases, describe those structures explicitly, and estimate the extent of failure of surjectivity of the Galois correspondence for those structures.

Contents

1. Introduction

In 1969, Chase and Sweedler [5] defined the notion of a Hopf Galois extension of fields by abstracting the formal properties of a classical Galois extension of fields. In 1987, Greither and Pareigis [13] discovered that a classical Galois extension L/K of fields with Galois group G could also be a Hopf Galois extension for a K-Hopf algebra H other than $H = KG$, the group ring of the Galois group, acting in the obvious way on L. They showed that

Received August 6, 2019.

1991 *Mathematics Subject Classification.* 13B05, 12F10, 20B35, 13M05.

Key words and phrases. Finite commutative nilpotent algebras, abelian Hopf Galois extensions of fields, regular subgroups of finite affine groups.

ISSN 1076-9803/2019

determining the number of Hopf Galois structures on L/K depends solely on the Galois group G. More precisely, the Hopf Galois structures correspond to regular subgroups N of the permutation group of G that are normalized by the image $\lambda(G)$ of the left regular representation of G in $\mathrm{Perm}(G)$. In many examples the subgroup N of $\mathrm{Perm}(G)$ need not be isomorphic to G, so we define the *type* of the Hopf Galois extension of L/K corresponding to N to be the isomorphism class of the group N.

Since the appearance of [13] there has been a fairly steady sequence of papers studying the number of Hopf Galois structures on a Galois extension of fields L/K with Galois group G. These range from Byott's uniqueness paper [2] and his theorem [3] that if G is a non-abelian simple group then L/K has exactly two Hopf Galois structures, to papers that for suitable Galois groups G describe large numbers of Hopf Galois structures on L/K, e.g. [7], or describe Hopf Galois structures of all possible types, e. g. [1].

Counting Hopf Galois structures on a field extension with Galois group G is often made easier by translating the problem of finding regular subgroups of $\mathrm{Perm}(G)$ that are isomorphic to a given group N and are normalized by $\lambda(G)$ to a problem of finding regular subgroups of $\mathrm{Hol}(N)$ that are isomorphic to G. This translation from $\mathrm{Perm}(G)$ to $\mathrm{Hol}(N)$ was first codified in [2], and has been the approach of choice for most papers devoted to counting Hopf Galois structures.

In [4] and subsequently in [12] Caranti, et. al. showed that for a finite abelian p-group, any commutative regular subgroup of $\mathrm{Hol}(G)$ can be obtained as the circle, or adjoint, group of a commutative nilpotent algebra structure $(G, +, \cdot)$ on the additive group G. Meanwhile, Rump [15] defined a left brace and showed that if $(A, +, \cdot)$ is a radical ring, then $(A, \circ, +)$ is a left brace, and Guarneri and Vendramin [14] extended the concept to that of a skew left brace by relaxing the commutativity assumption on the operation $+$. In particular, they characterized skew braces as follows:

Theorem 1.1. *Let $(B, \circ, \star)$ be a set with two group operations $\circ$ and $\star$. Let $\lambda_\circ, \lambda_\star : B \to \mathrm{Perm}(B)$ be the two left regular representation maps, defined by $\lambda_\circ(b)(x) = b \circ x$, $\lambda_\star(b)(x) = b \star x$. Let $\mathrm{Hol}(B, \star) \subset \mathrm{Perm}(B)$ be the normalizer of $\lambda_\star(B)$ in $\mathrm{Perm}(B)$. Then B is a skew left brace if and only if $\lambda_\circ(B) \subset \mathrm{Hol}(B, \star)$.*

Subsequently, Byott and Vendramin [16] showed that $(B, \circ, \star)$ is a skew left brace if and only if there exists a Galois extension L/K with Galois group G and a Hopf Galois structure of type N so that $G \cong (B, \circ)$ and $N \cong (B, \star)$. Their observation follows from the fact from Greither-Pareigis that if $N = (B, \star)$ is normalized by $\lambda_\circ(B) = \lambda(G)$ in $\mathrm{Perm}(G)$, then N corresponds to a Hopf Galois structure on L/K, and conversely, if L/K is G-Galois and has a Hopf Galois structure corresponding to the regular subgroup N of $\mathrm{Perm}(G)$ normalized by $\lambda_\circ(G)$ in $\mathrm{Perm}(G)$, then N defines a new group structure $(G, \star) \cong N$ on G which makes $(G, \circ, \star)$ into a skew brace.

To illustrate the richness of Hopf Galois structures, especially on Galois extensions with Galois group an elementary abelian p-group, insights can be gained by just looking at those arising from nilpotent $\mathbb{F}_p$-algebras. In this paper we look at Hopf Galois structures corresponding to a class of commutative nilpotent $\mathbb{F}_p$-algebras A of $\mathbb{F}_p$-dimension n that are "almost" trivial. Thus we assume that A has the property that $\dim_{\mathbb{F}_p}(A^2) = 1$ and $A^3 = 0$. If $A^2 = 0$, then the Hopf Galois structure on a Galois extension with Galois group $G \cong (A, +)$ is unique, namely that given by the Galois group, so our examples of nilpotent algebras are about as close to being trivial as possible.

We determine the isomorphism types of commutative nilpotent $\mathbb{F}_p$-algebras A of dimension n with $A^3 = 0$ and $\dim(A^2) = 1$, and determine the number of regular subgroups of $\mathrm{Hol}(G)$ associated to each isomorphism type. For $n = 4$ this approach yields more than p^9 regular subgroups. We describe the Hopf Galois structure on L/K corresponding to each regular subgroup arising from a given isomorphism type of algebra. We also explicitly describe the Hopf algebra action on L/K, and estimate the extent of failure of the Galois correspondence for the Hopf Galois structure to map onto the intermediate fields between K and L.

Throughout, let L/K be a Galois extension of fields with Galois group Γ, an elementary abelian p-group of order p^n, p an odd prime. For a finite abelian p-group G with operation $+$, a ring structure $A = (G, +, \cdot)$ on G will be called nilpotent if A is associative and nilpotent: $A^m = 0$ for some $m > 1$.

This research was inspired by discussions with Tim Kohl. Many thanks to him for sharing his enthusiasm with me. My thanks also to the referee for some insightful comments.

2. Hopf Galois structures from nilpotent algebras

Let $A = (A, +, \cdot)$ be a nilpotent $\mathbb{F}_p$-algebra of $\mathbb{F}_p$-dimension n. The circle operation $\circ$ on A, defined by $a \circ b = a + b + a \cdot b$ for a, b in A, is clearly associative with identity element 0. Since A is nilpotent, the circle inverse $\overline{a}$ of a is

$$\overline{a} = -a + a^2 - a^3 + \dots,$$

where $a^r = a \cdot a \cdot \ldots \cdot a$ (r factors), and so $(A, \circ)$ is a group, the adjoint group of A. It is well known since [15] that then $(A, \circ, +)$ is a left brace with additive group $(A, +)$, that is, for all a, b, c in A

$$a \circ (b + c) = a \circ b - a + a \circ c.$$

Let $A^n = \{a_1 \cdot a_2 \cdot \ldots \cdot a_n : a_1, \ldots, a_n \text{ in } A\}$. Then we have

Proposition 2.1. *Let $(A, +)$ be an abelian p-group of finite order p^n, and let $(A, +, \cdot)$ be a nilpotent ring structure on $(A, +)$. Let $(A, \circ)$ be the adjoint group on A and let $\lambda_+, \lambda_\circ$ be the corresponding left regular representations of A into* $\mathrm{Perm}(A)$*. Then the following are equivalent:*

(i) $\lambda_\circ(A)$ *is normalized by* $\lambda_+(A)$.
(ii) $A^3 = 0$.
(iii) $(A, \circ, +)$ *is a left skew brace with* $(A, \circ)$ *acting as the additive group.*

In [9] a skew brace satisfying (iii) was called a bi-skew brace.

The equivalence of (i) and (iii) follows by the Guarneri-Vendramin characterization, Theorem 1.1 above. The equivalence of (ii) and (iii) is Proposition 4.1 of [9], a routine computation working modulo A^4. As the referee kindly pointed out, the equivalence of (i) and (ii) for finite dimensional nilpotent algebras over a field was observed immediately following Lemma 3 in [4].

We identify the corresponding Hopf Galois structures:

Corollary 2.2. *Let L/K be a Galois extension with Galois group $(A, +) = G$, an abelian p-group of order p^n. Let $A = (A, +, \cdot)$ be a commutative nilpotent ring structure on $(A, +)$ and suppose $A^3 = 0$. Then $T = \lambda_\circ(A) \subset$* Perm$(A)$ *yields a Hopf Galois structure on L/K by a K-Hopf algebra H, where*

i) H is the fixed ring of LT under the action of G:

$$H = LT^G = \left\{ \sum_{x \in G} b_x \lambda_\circ(x) : b_{x - x\cdot z} = b_x^z \textit{ for all } z \textit{ in } G \right\};$$

ii) H acts on L by

$$\left(\sum_{x \in G} b_x \lambda_\circ(x) \right)(a) = \sum_{x \in G} b_x a^{-x+x^2}$$

for b, a in L.

Proof. Let $\{e_z : z \in G\}$ be the dual basis to the basis $G = (A, +)$ of the group ring $L[G]$. The action of $T = \lambda_\circ(A)$ on $GL = \sum_{z \in G} Le_z$ is by

$$\lambda_\circ(x)(e_z) = e_{x \circ z}$$

for x in G. This yields an action of the group ring LT on GL making GL an LT-Hopf Galois extension of L. Since $\lambda_+(G)$ acts on T by

$$\lambda_+(z)\lambda_\circ(x)\lambda_+(-z) = \lambda_\circ(x - x \cdot z),$$

the corresponding K-Hopf algebra is

$$H = LT^G = \left\{ \sum_{x \in G} b_x \lambda_\circ(x) : b_{x - x\cdot z} = b_x^z \text{ for all } z \text{ in } G \right\}$$

where for a in L and y in G, a^y is the image of a under the Galois action of y on L, and H acts on GL by

$$\left(\sum_{x \in G} b_x \lambda_\circ(x) \right) \left(\sum_{y \in G} a_y e_y \right) = \sum_{x, y \in G} b_x a_y e_{x \circ y}.$$

Now L embeds in GL by

$$a \mapsto \sum_{y\in G} a^y e_y.$$

So the action of H on L is by

$$\left(\sum_{x\in G} b_x \lambda_\circ(x)\right)(a) = \sum_{x,y\in G, x\circ y=0} b_x a^y.$$

Since $x^3 = 0$, $x \circ (-x + x^2) = 0$, and so the action of H on L can be written

$$\left(\sum_{x\in G} b_x \lambda_\circ(x)\right)(a) = \sum_{x\in G} b_x a^{-x+x^2}.$$

□

There is no a priori reason why $(A, \circ)$ and hence $T = \lambda_\circ(A)$ should be isomorphic to G, so that H has type G. But if A is commutative, it is true: we note the following variant of Theorem 1 of [12]:

Proposition 2.3. *Let $p > 3$ be an odd prime and $G = (G, +)$ be a finite abelian p-group of order p^n. Let $A = (G, +, \cdot)$ be a commutative nilpotent ring structure on $(G, +)$ and suppose $A^3 = 0$. Then the regular subgroup $N = (G, \circ)$ of* $\mathrm{Hol}(G) \subset \mathrm{Perm}(G)$ *is isomorphic to $(G, +)$.*

The statement of Theorem 1 of [12] replaces the condition $A^3 = 0$ in Proposition 2.3 by the condition that the p-rank m of G should satisfy $m + 1 < p$. The proof of Proposition 2.3 is essentially the same as that of Theorem 1 of [12]. The only change is that the condition $A^3 = 0$ implies that $a^p = 0$ for all a in A, which slightly simplifies the proof in [12]] by eliminating the need to apply a condition on the p-rank of G to insure that a^p does not interfere with the induction argument.

3. Working in the affine group

For the remainder of the paper we restrict G to be an elementary abelian p-group of p-rank $n > 1$, and we consider only commutative nilpotent ring structures A on $(G, +)$ with $A^3 = 0$. From [7], it is known that the number of isomorphism types of such structures is bounded from below by p^b where $b = O(n^3)$.

Each such ring is an $\mathbb{F}_p$-algebra. Let $\dim_{\mathbb{F}_p} A/A^2 = r$ and $\dim_{\mathbb{F}_p} A^2 = n-r$. Given an $\mathbb{F}_p$-basis $(x_1, \ldots, x_r)$ of A/A^2 and a basis $(y_1, \ldots y_{n-r})$ of A^2, the multiplicative structure of A with those bases is given by a set $\Phi^{(k)} = (\phi^{(k)}_{ij})$ of $r \times r$ symmetric matrices with coefficients in $\mathbb{F}_p$, by the equations

$$x_i x_j = \sum_{k=1}^{n-r} \phi^{(k)}_{i,j} y_k.$$

The group structure $(G, \circ)$ on G arising from $(A, +, \cdot)$ depends on the matrices $\{\Phi^{(k)}\}$, and hence so does the regular subgroup $T = \lambda_\circ(G)$ of $\mathrm{Perm}(G)$.

It is convenient to view $\mathrm{Hol}(G)$ as the affine group $\mathrm{Aff}_n(\mathbb{F}_p)$ and realize the regular subgroup T inside $\mathrm{Aff}_n(\mathbb{F}_p)$.

Let $\mathrm{Aff}_n(\mathbb{F}_p)$ be the subset of $\mathrm{GL}_{n+1}(\mathbb{F}_p)$ consisting of matrices of the form

$$\begin{pmatrix} B & v \\ 0 & 1 \end{pmatrix},$$

where B is an $n \times n$ matrix, v is a column vector in $\mathbb{F}_p^n$, 0 is a n-row vector of zeros and 1 is a 1×1 identity matrix. Then $\mathrm{Aff}_n(\mathbb{F}_p)$ may be identified as the holomorph $\mathrm{Hol}(\mathbb{F}_p^n) = \lambda(\mathbb{F}_p^n) \cdot \mathrm{Aut}(\mathbb{F}_p^n)$ of the additive group $\mathbb{F}_p^n$, where the matrices

$$\begin{pmatrix} P & 0 \\ 0 & 1 \end{pmatrix}$$

with P in $\mathrm{GL}_n(\mathbb{F}_p)$ form the subgroup $\mathrm{Aut}(\mathbb{F}_p^n)$ of $\mathrm{Hol}(\mathbb{F}_p^n)$, and matrices

$$\begin{pmatrix} I & x \\ 0 & 1 \end{pmatrix}$$

for x in $\mathbb{F}_p^n$ form the subgroup $\lambda(\mathbb{F}_p^n)$.

The group $T = \lambda_\circ(A)$ embeds as a regular subgroup of $\mathrm{Aff}_n(\mathbb{F}_p)$ as follows:

The map $\lambda_\circ$ from $\mathbb{F}_p^n$ to $\mathbb{F}_p^n$ is given by $\lambda_\circ(x)(y) = x \circ y = x + y + x \cdot y$. Write $\lambda_\circ(x)(y) = x + y + L_x(y)$, where $L_x(y) = x \cdot y$. Then L_x is a linear function from $\mathbb{F}_p^n$ to $\mathbb{F}_p^n$, so has a matrix relative to the standard basis of $\mathbb{F}_p^n$ that we also call L_x. Then $\lambda_\circ(x)$ in $\mathrm{Aff}_n(\mathbb{F}_p)$ becomes the $n + 1 \times n + 1$ matrix

$$T_x = \begin{pmatrix} I + L_x & x \\ 0 & 1 \end{pmatrix},$$

because for any y in $\mathbb{F}_p^n$, we have

$$T_x \begin{pmatrix} y \\ 1 \end{pmatrix} = \begin{pmatrix} y + L_x(y) + x \\ 1 \end{pmatrix} = \begin{pmatrix} y + x \cdot y + x \\ 1 \end{pmatrix} = \begin{pmatrix} \lambda_\circ(x)(y) \\ 1 \end{pmatrix}.$$

4. The case $r = n - 1$

We now look at the class of examples where $\dim(A) = n, \dim(A^2) = 1, A^3 = 0$. Then A has the $\mathbb{F}_p$-basis $(x_1, \ldots, x_{n-1}, x_n)$ with $x_i x_j = \phi_{i,j} x_n$, so A is determined by that basis and the single $n \times n$ structure matrix $\Phi = (\phi_{ij})$. Since $A^3 = 0$, $\phi_{ni} = \phi_{in} = 0$ for all i. In this section we determine the regular subgroups of $\mathrm{Aff}_n(\mathbb{F}_p)$ associated to A.

Since A is commutative, the structure matrix Φ is symmetric. Then (c.f. [17], Section 3.4.6) there is an invertible matrix P so that $P\Phi P^T = D = \mathrm{diag}(D_s, 0)$ is diagonal, where $D_s = \mathrm{diag}(1, \ldots, 1, s)$ is $k \times k$ for some $k \leq n$, where s is either 1 or any chosen non-square in $\mathbb{F}_p$.

So set $z = Px$. Then $z_n = x_n$ and with respect to the basis $(z_1, \ldots, z_{n-1}, z_n)$, A has the structure matrix D with $z_i z_j = d_{ij} z_n$ and

$$D = \operatorname{diag}(d_1, \ldots, d_n) = \operatorname{diag}(1, 1, \ldots, 1, s, 0, \ldots 0)$$

with $s = d_k$.

So by that change of basis of A, we can realize the group T conveniently in

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

by picking the basis $(z_1, \ldots, z_n)$ for A so that $\Phi = D$.

Let $\{e_1, \ldots, e_n\}$ be the standard basis of $\mathbb{F}_p^n$ corresponding to the basis $\{z_1, \ldots z_n\}$ of $A = (A, +)$. Then $\lambda_\circ(z_i) = T_i$ is the element

$$T_i = \begin{pmatrix} L_i & e_i \\ 0 & 1 \end{pmatrix},$$

which acts on $A = \{r = \sum_{i=1}^n r_i e_i : r \in \mathbb{F}_p^n\}$ embedded as elements $\binom{r}{1}$ in $\mathbb{F}_p^{n+1}$ by

$$\begin{pmatrix} L_i & e_i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} e_j \\ 1 \end{pmatrix} = \begin{pmatrix} e_i \circ e_j \\ 1 \end{pmatrix} = \begin{pmatrix} e_i + e_j \\ 1 \end{pmatrix} \text{ for } i \neq j$$
$$\begin{pmatrix} L_i & e_i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} e_i \\ 1 \end{pmatrix} = \begin{pmatrix} e_i \circ e_i \\ 1 \end{pmatrix} = \begin{pmatrix} e_i + e_i + d_i e_n \\ 1 \end{pmatrix}.$$

5. The number of Hopf Galois structures associated to A

In this section we determine the number of Hopf Galois structures on a Galois extension L/K of fields with Galois group $G = (\mathbb{F}_p^n, +)$ that correspond to certain isomorphism types of nilpotent algebra structures on G.

To do so, we have

Proposition 5.1. *Let A be a nilpotent $\mathbb{F}_p$-algebra structure on $(\mathbb{F}_p^n, +)$. Then the number of Hopf Galois structures on L/K corresponding to the isomorphism type of A is equal to*

$$|\operatorname{GL}_n(\mathbb{F}_p)|/|\operatorname{Sta}(T)|$$

where $T = \lambda_\circ(A)$ is the regular subgroup of $\operatorname{Aff}_n(\mathbb{F}_p)$ corresponding to A and

$$\operatorname{Sta}(T) = \{P \in \operatorname{GL}_n(\mathbb{F}_p) : \begin{pmatrix} P & 0 \\ 0 & 1 \end{pmatrix} T = T \begin{pmatrix} P & 0 \\ 0 & 1 \end{pmatrix}.$$

This follows by [4], which showed that two nilpotent $\mathbb{F}_p$-algebras on $(\mathbb{F}_p^n, +)$ are isomorphic if and only if the corresponding regular subgroups of $\operatorname{Aff}_n(\mathbb{F}_p)$ are conjugate by an element of $\operatorname{Aut}(G) = \begin{pmatrix} \operatorname{GL}_n(\mathbb{F}_p) & 0 \\ 0 & 1 \end{pmatrix}$ in $\operatorname{Aff}_n(\mathbb{F}_p)$.

We note that given a regular subgroup T of $\operatorname{Aff}_n(\mathbb{F}_p)$ normalized by $\lambda_+(A)$, corresponding to A with $A^3 = 0$, then all of the regular subgroups in the orbit of T under conjugation by $\operatorname{Aut}(G)$ correspond to algebras A_1

isomorphic to A, hence have $A_1^3 = 0$. Thus all are normalized by $\lambda(G)$. Hence by Galois descent, all of those regular subgroups give rise to Hopf Galois structures on a Galois extension L/K with Galois group G.

The commutative nilpotent $\mathbb{F}_p$-algebra A with $A^2 = 0$ yields the classical Galois structure on a Galois extension with Galois group G. For then $\Phi = D = 0$, and the corresponding regular subgroup T of $\mathrm{Aff}_n(\mathbb{F}_p)$ is $\lambda_+(A)$, which is stable under conjugation by every element of $\mathrm{Aut}(G)$, hence yields only the classical Galois structure on L/K.

Since p is odd, we may assume that $\Phi = \mathrm{diag}(D_s, 0)$. Let

$$\begin{aligned} \overline{v}_s &= (r_1, r_2, \dots, r_{k-1}, sr_k)^T, \\ \overline{v} &= (r_1, r_2, \dots, r_{k-1}, r_k)^T, \\ \overline{w} &= (r_{k+1}, \dots, r_{n-1})^T \end{aligned}$$

(column vectors of elements of $\mathbb{F}_p$). Then it is convenient to write elements of $T = \lambda_\circ(A)$ as block matrices of the form

$$T = \{\lambda_\circ(r) = \begin{pmatrix} I & 0 & 0 & \overline{v} \\ 0 & I & 0 & \overline{w} \\ \overline{v}_s^T & 0 & 1 & r_n \\ 0 & 0 & 0 & 1 \end{pmatrix} : r \in \mathbb{F}_p^n\}$$

where the diagonal entries are identity matrices of size $k \times k$, $(n-1-k) \times (n-1-k)$, 1×1 and 1×1, respectively.

To determine the number of Hopf Galois structures corresponding to regular subgroups in the orbit of T, we need to find the stabilizer of T under conjugation by the elements of $\mathrm{Aut}(G) = \mathrm{GL}_n(\mathbb{F}_p)$.

To determine the stabilizer of T, we seek the set of $(n+1) \times (n+1)$ matrices

$$Q = \begin{pmatrix} P & 0 \\ 0 & 1 \end{pmatrix}$$

in $\mathrm{Aut}(G) \subset \mathrm{Aff}_n(G)$ so that $QTQ^{-1} = T$, where P in $\mathrm{GL}_n(\mathbb{F}_p)$ has the form

$$P = \begin{pmatrix} P_{11} & P_{12} & P_{13} \\ P_{21} & P_{22} & P_{23} \\ P_{31} & P_{32} & P_{33} \end{pmatrix}$$

with blocks of the same size as $\lambda_\circ(r)$. Let $\lambda_\circ(r')$ be another element of T. We compute $P\lambda_\circ(r)$ and $\lambda_\circ(r')P$ and set $P\lambda_\circ(r) = \lambda_\circ(r')P$.

Equating the (11) terms yields that $P_{13} = 0$.

Equating the (21) terms yields that $P_{23} = 0$.

Equating the (32) terms yields that $P_{12} = 0$.

Then equating the (31) terms yields

$$\overline{v}_s'^T P_{11} = P_{33}\overline{v_s}^T.$$

Equating the (14) terms yields

$$P_{11}v = v'.$$

Equating the (24) terms yields

$$w' = P_{21}v + P_{22}w.$$

Equating the (34) terms yields

$$t' = P_{31}v + P_{32}w + P_{33}t.$$

The (24) and (34) equations define w' and t'. Setting $P_{33} = q$, a non-zero element of $\mathbb{F}_p$, then from (14) and (31) we have

$$P_{11}^T v_s' = qv_s \text{ and } P_{11}v = v'.$$

Recalling that $D_s = \mathrm{diag}(1, \dots 1, s)$, a $k \times k$ matrix, then $D_s v = v_s$, $D_s v' = v_s'$. So

$$P_{11}^T D_s v' = qD_s v,$$

hence

$$P_{11}^T D_s P_{11} v = qD_s v.$$

Thus P is in the stabilizer of T if

$$P = \begin{pmatrix} P_{11} & 0 & 0 & 0 \\ P_{21} & P_{22} & 0 & 0 \\ P_{31} & P_{32} & P_{33} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

where

$P_{33} = q$ is in $\mathrm{GL}_1(\mathbb{F}_p)$;
P_{32} is $1 \times (n-1-k)$ and arbitrary;
P_{31} is $1 \times k$ and arbitrary;
P_{22} is in $\mathrm{GL}_{n-1-k}(\mathbb{F}_p)$;
P_{21} is $(n-1-k) \times k$ and is arbitrary; and
P_{11} is in $\mathrm{GL}_k(\mathbb{F}_p)$ and satisfies $P_{11}^T D_s P_{11} = qD_s$.

As noted above, we may assume that A has a basis for which A has the structure matrix $D = \begin{pmatrix} D_s & 0 \\ 0 & 0 \end{pmatrix}$ where $D_s = \mathrm{diag}(1, 1, \dots, s)$ is $k \times k$, $k < n$. To determine the possible P_{11} we have three cases:

(1) k is odd;
(2) k is even and $s = 1$
(3) k is even and s is a non-square in $\mathbb{F}_p$.

Each case involves a different orthogonal group. The notation for the orthogonal groups over $\mathbb{F}_p$ is from [17], Section 3.7.

Proposition 5.2. *For Case 1), let $k = 2m + 1$. For all $q \neq 0$ in $\mathbb{F}_p$, there exists a $k \times k$ matrix C so that $C^T C = qI$ if and only if q is a square. Fixing C, then for any s in $\mathbb{F}_p$, $P_{11}^T D_s P_{11} = qD_s$ if and only if $P_{11} = CU$ for U in $\mathrm{GO}_{2m+1}(\mathbb{F}_p)$.*

For Case 2), let $k = 2m$ and $s = 1$. For all $q \neq 0$ in $\mathbb{F}_p$, there exists a $k \times k$ matrix C so that $C^T C = qI$. Fixing C, then $P_{11}^T P_{11} = qI$ if and only if $P_{11} = CU$ for U in $\mathrm{GO}_{2m}^+(\mathbb{F}_p)$.

For Case 3), let $k = 2m$ and s be a non-square in $\mathbb{F}_p$. For all $q \neq 0$ in $\mathbb{F}_p$, there exists a $k \times k$ matrix C so that $C^T D_s C = qD_s$. Fixing C, then $P_{11}^T D_s P_{11} = qD_s$ if and only if $P_{11} = CU$ for U in $\mathrm{GO}_{2m}^-(\mathbb{F}_p)$.

Proof. In Case 1) with k odd, if there exists C so that $C^T C = qI$, then taking determinants gives $\det(C)^2 = q^k$, hence q must be a square.

For the rest, it suffices to find the matrix C in each case.

For Case 1), let $q = t^2$, then $C = tI$ satisfies $C^T C = qI$.

For Case 2), let $q = f^2 + g^2$, let $Q = \begin{pmatrix} f & g \\ -g & f \end{pmatrix}$ and let $C = \mathrm{diag}(Q, Q, \dots, Q)$. Then $C^T C = qI$.

For Case 3), let $q = f^2 + g^2$ and Q as in Case 2). For s a non-square in $\mathbb{F}_p$, find w and x in $\mathbb{F}_p$ so that $w^2 + sx^2 = q$. (If q is a square, let $x = 0, w^2 = q$; if q is a non-square, let $w = 0$ and find x so that $sx^2 = q$, possible because the squares have index 2 in $\mathbb{F}_p^\times$.) Then $R = \begin{pmatrix} w & sx \\ x & -w \end{pmatrix}$ satisfies $R^T \begin{pmatrix} 1 & 0 \\ 0 & s \end{pmatrix} R = \begin{pmatrix} q & 0 \\ 0 & sq \end{pmatrix}$. Let $C = \mathrm{diag}(Q, Q, \dots, Q, R)$. Then $C^T D_s C = qD_s$. □

Corollary 5.3. *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) $k = 2m + 1$

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, and hence the number of Hopf Galois structures on L/K associated to the isomorphism type of A, is

1)

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

2)

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

3)

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

The orders of the $k \times k$ orthogonal groups are polynomials in p of degree $(k^2 - k)/2$ (c.f. [17], p. 72), and the order of $\mathrm{GL}_n(\mathbb{F}_p)$ is a polynomial of degree n^2. Hence we have

Corollary 5.4. *Let A be a commutative nilpotent $\mathbb{F}_p$-algebra of dimension n with $A^3 = 0$, $\dim(A^2) = 1$ and structure matrix of rank k. Let L/K be a*

Galois extension with Galois group $G \cong (A, +)$. Then the number of Hopf Galois structures on L/K of type $(A, \circ)$ is a polynomial function of p of degree

$$n^2 - (k^2 - k)/2 - (n-k)(n-1) - 1 = \frac{(2n-k)(k+1)}{2} - 1.$$

The number of Hopf Galois structures increases with k and is maximal when $k = n - 1$.

6. The cases $n = 2, 3, 4$

We compare the counts of Hopf Galois structures in the last section to the number of Hopf Galois structures found by formal group methods in [6] for $n = 2, 3$.

The case $n = 2$. Let $n = 2, k = 1$. Then $\Phi = (1)$. For P to stabilize T,

$$P = \begin{pmatrix} P_{11} & 0 \\ P_{21} & P_{22} \end{pmatrix},$$

and the number of choices for each submatrix in P is

$$\begin{pmatrix} |\mathrm{GO}_1| & 1 \\ p & \frac{p-1}{2} \end{pmatrix}.$$

Since $\mathrm{GO}_1 = \{(1), (-1)\}$, the size of the stabilizer of the regular subgroup is

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

The order of $GL_2(\mathbb{F}_p)$ is $(p^2-1)(p^2-p)$. So there are $p^2 - 1$ distinct regular subgroups in the orbit of the regular subgroup corresponding to Φ.

Since every nilpotent algebra structure A on $(\mathbb{F}_p^2, +)$ has $A^3 = 0$, we have counted all Hopf Galois structures on a Galois extension with Galois group C_p^2.

The case $n = 3$.

Subcase: $k = 1$: The matrix P is in the stabilizer of the regular subgroup T corresponding to $\Phi = \mathrm{diag}(1, 0)$ if

$$P = \begin{pmatrix} P_{11} & 0 & 0 \\ P_{21} & P_{22} & 0 \\ P_{31} & P_{32} & P_{33} \end{pmatrix},$$

all submatrices being 1×1. So the number of choices for each entry is

$$\begin{pmatrix} |\mathrm{GO}_1| & 1 & 1 \\ p & |\mathrm{GL}_1| & 1 \\ p & p & \frac{p-1}{2} \end{pmatrix}.$$

Then $|\mathrm{GO}_1| = 2$ and $|\mathrm{GL}_1| = p - 1$, so the size of the stabilizer $\mathrm{Sta}(T)$ is

$$p^3(p-1)^2,$$

and the orbit has cardinality

$$|\mathrm{GL}_3(\mathbb{F}_p)|/|\mathrm{Sta}(T)| = (p-1)^3(p+1).$$

Subcase: $k=2$, $s=1$, $\Phi = \mathrm{diag}(1,1)$: The matrix P is in the stabilizer if

$$P = \begin{pmatrix} P_{11} & 0 \\ P_{21} & P_{22} \end{pmatrix},$$

where P_{11} is in GO_2^+. The number of choices for each submatrix is

$$\begin{pmatrix} |\mathrm{GO}_2^+| & 1 \\ p^2 & p-1 \end{pmatrix},$$

and $|\mathrm{GO}_2^+| = 2(p-1)$, so the size of the stabilizer is

$$2(p-1)^2p^2.$$

Subcase: $k=2$, s a non-square, $\Phi = \mathrm{diag}(1,s)$: The matrix P is in the stabilizer if

$$P = \begin{pmatrix} P_{11} & 0 \\ P_{21} & P_{22} \end{pmatrix},$$

where P_{11} is in GO_2^-. The number of choices for each submatrix is

$$\begin{pmatrix} |\mathrm{GO}_2^-| & 1 \\ p^2 & p-1 \end{pmatrix},$$

and $|\mathrm{GO}_2^-| = 2(p+1)$, so the size of the stabilizer is

$$2(p^2-1)p^2.$$

The number of regular subgroups corresponding to each case is $|\mathrm{GL}_3|$ divided by the order of the stabilizer:

For $k=1$, the number of regular subgroups is

$$(p^3-1)(p+1).$$

For $k=2, s=1$, the number of regular subgroups is

$$(p^3-1)p(p+1)/2.$$

For $k=2, s$ a non-square, the number of regular subgroups is

$$(p^3-1)p(p-1)/2.$$

These agree with the counts found in [6].

The only isomorphism type of nilpotent algebras $A = (\mathbb{F}_p^3, +, \cdot)$ for which $A^3 \neq 0$ is the algebra with $\dim(A/A^2) = 1$.

The case $n = 4$. This case has not previously been looked at.

For $n = 4$ there are four subcases:

$k = 1$. Here

$$P = \begin{pmatrix} P_{11} & 0 & 0 \\ P_{21} & P_{22} & 0 \\ P_{31} & P_{32} & P_{33} \end{pmatrix},$$

where P_{22} is 2×2. The number of choices for each submatrix is

$$\begin{pmatrix} |\mathrm{GO}_1| & 1 & 1 \\ p^2 & |\mathrm{GL}_2| & 1 \\ p & p^2 & \frac{p-1}{2} \end{pmatrix}.$$

So the size of the stabilizer is

$$2p^5(p^2-1)(p^2-p)\left(\frac{p-1}{2}\right).$$

$k = 2, s = 1$: Here P_{11} is 2×2. The number of choices for each matrix is

$$\begin{pmatrix} |\mathrm{GO}_2^+| & 1 & 1 \\ p^2 & |\mathrm{GL}_1| & 1 \\ p^2 & p & p-1 \end{pmatrix}.$$

So the size of the stabilizer is

$$2p^5(p-1)^3.$$

$k = 2$, s a non-square. It is the same as the last case except P_{11} is in GO_2^-, so the size of the stabilizer is

$$2p^5(p-1)^2(p+1).$$

$k = 3$. Here

$$P = \begin{pmatrix} P_{11} & 0 \\ P_{21} & P_{22} \end{pmatrix}$$

where P_{11} is in GO_3, which has order $2p(p^2-1)$, and $P_{22} = (q)$ where q is a square. So the order of the stabilizer is

$$2p(p^2-1)p^3\frac{p-1}{2}.$$

The number of regular subgroups in each case is the order of $\mathrm{GL}_4(\mathbb{F}_p)$ divided by the orders of the respective stabilizers:

Case	number of regular subgroups
$k = 1$	$(p^2+1)(p+1)(p^3-1)$
$k = 2, s = 1$	$p(p^2+1)(p^3-1)(p+1)^2/2$
$k = 2, s$ a non-square	$p(p^4-1)(p^3-1)/2$
$k = 3$	$p^2(p^4-1)(p^3-1)$

The total number of Hopf Galois structure exceeds p^9. Note that the degrees of the polynomials in each case agree with Corollary 5.4.

The Hopf Galois structure. Given a Galois extension L/K with Galois group $G \cong \mathbb{F}_p^n$, if the commutative nilpotent algebra A with $\dim(A^2) = 1, A^3 = 0$ has diagonal structure matrix $\Phi = \mathrm{diag}(d_1, \ldots, d_k, 0, \ldots,)$, then the regular subgroup T corresponding to D acts on GL by

$$\lambda_\circ(r)(e_t) = e_{r \circ t} = e_w$$

where

$$w = r + t + \left(\sum_{i=1}^{k} r_i t_i d_i\right) x_n,$$

and $\lambda(G)$ conjugates T by

$$\lambda(t)\lambda_\circ(r)\lambda(-t) = \lambda_\circ(r - r \cdot t) = \lambda_\circ\left(r - \sum_{i=1}^{k} r_i t_i d_i) x_n\right).$$

7. The Galois correspondence ratio

Let A be a commutative $\mathbb{F}_p$-algebra of dimension n with $A^3 = 0$, yielding the skew brace $(A, +, \circ)$. In [8] (generalized in [9] and [10]) we showed that for a Galois extension L/K with Galois group $(A, +)$ and an H-Hopf Galois structure of type $(A, \circ)$, the image of the Galois correspondence for the Hopf Galois structure is in bijective correspondence with the ideals of A. Thus the Galois correspondence ratio for the Hopf Galois structure is

$$GC(L/K, (A, +), H) = \frac{|\{\text{ ideals of } A\}|}{|\{\text{ subgroups of } (A, +)\}|}.$$

We have

Proposition 7.1. *Let A be as in Corollary 5.3 with a non-zero structure matrix D_s of rank $k \geq 1$. Let L/K be a Galois extension with Galois group $G \cong (A, +)$ and a Hopf Galois structure associated to the skew brace $(A, +, \circ)$. Then*

$$GC(L/K, (A, +), H) = O\left(\frac{1}{p^{(n-1)/2}}\right) \text{ for } n \text{ odd;}$$
$$= O\left(\frac{1}{p^{n/2}}\right) \text{ for } n \text{ even.}$$

Proof. The denominator of $GC(L/K, (A, +), H)$ is equal to the number of subspaces of $\mathbb{F}_p^n$, a known quantity. So to estimate this ratio, we need to estimate the number of ideals of A.

The algebra $A = (A, n, k)$ has basis $(x_1, x_2, \ldots, x_n)$ where $x_i^2 = x_n$ for $i = 1, 2, \ldots, k-1$, $x_k^2 = s \neq 0$ and $x_i^2 = 0$ for $k < i \leq n$. Viewing A as a vector space with basis $x_1, \ldots x_n$, we know (c.f [11], Section 1) that the number of subspaces of $\mathbb{F}_p^n$ of dimension k is $\geq p^{k(n-k)}$ and has order of magnitude $= p^{k(n-k)}$.

We can count the total number of subspaces of A by viewing the subspaces of A as row spaces of $n \times n$ matrices with entries in $\mathbb{F}_p$ and counting the number of parameters of all possible reduced row echelon forms of those $n \times n$ matrices. So let $R = (c_1, c_2, \dots, c_r)$ denote the general reduced row echelon form of rank r with r non-zero rows and pivots in columns numbered $c_1, c_2, \dots, c_r$. Then the number n_R of $\mathbb{F}_p$-parameters in the matrix $R = (c_1, c_2, \dots, c_r)$, (counting row by row from the top) is equal to

$$(c_2 - c_1 - 1) + 2(c_3 - c_2 - 1) + \dots + \dots + (r-1)(c_r - c_{r-1} - 1) + r(n+1-c_r-1).$$

So the dimension of the subspace defined by the matrix R is

$$\begin{aligned} m_R &= p^{n_R} \\ &= p^{c_2-c_1-1} \cdot p^{2(c_3-c_2-1)} \cdot \dots \cdot p^{(r-1)(c_r-c_{r-1}-1)} \cdot p^{r(n+1-c_r-1)}. \end{aligned}$$

The largest m_R can be is if $(c_1, c_2, \dots, c_r) = (1, 2, \dots, r)$, so that the product reduces to the single term $p_r = p^{r(n+1-r-1)}$. Thus for n even, the number $s(\mathbb{F}_p^n)$of subspaces of $\mathbb{F}_p^n$ is a polynomial in p with a unique highest degree term, when $r = n/2$, namely $p^{n^2/4}$. For n odd, $s(\mathbb{F}_p^n)$ is a polynomial in p with two equal highest degree terms, when $r = (n-1)/2$ or $r = (n+1)/2$, namely $p^{(n^2-1)/4}$. Thus the leading term of $s(\mathbb{F}_p^n)$ for n odd is $= 2p^{(n^2-1)/4}$.

Now we estimate the number of ideals of A, assuming that in A, $x_1^2 = dx_n$ with $d \neq 0$. The key fact is that if a matrix R represents a subspace which is an ideal and contains an element $x = x_1 + a_2x_2 + \dots + a_nx^n$, then it also contains $x_1x = dx_n$. So R must contain a row $(0, 0, \dots, 0, 1)$. Thus the matrices

$$R = (1, 2, 3, \dots, r)$$

which give the largest number of parameters do not represent ideals, while the matrices

$$R_I = (1, 2, 3, \dots, r, n)$$

do represent ideals, but have r fewer parameters than R does. Also $R' = (2, 3, \dots r)$ represents an ideal if $x_2^2 = 0$, but R' has $n - r$ fewer parameters than R. In particular, for n odd, the matrix R_I giving the most parameters is

$$R_I = \left(1, 2, 3, \dots, \frac{n-1}{2}, n\right),$$

namely, $(n^2-1)/4$ parameters, and for n even, the matrix R_I giving the most parameters is

$$R_I = \left(1, 2, 3, \dots, \frac{n-1}{2}, n\right),$$

namely $n^2/4$.

Thus in the case of an A closest to the trivial algebra $A = (\mathbb{F}_p^n, +)$, the ratio

$$\#\{\text{ideals of } A\}/\#\{\text{subspaces of } A\} = O(1/(p^{(n-1)/2})) \text{ or } O(1/p^{n/2})$$

for n odd, resp. even. □

If A has $x_i^2 = s_i x_n$ for $s_i \neq 0$ for $i = 1, \ldots, d$, the number of subspaces that are ideals decreases as d increases, to the point where if $d = n-1$, then the ideals of A are the subspaces of A that contain x_n. Then the number of non-zero ideals of A is equal to the number of subspaces of $\mathbb{F}_p^{n-1}$.

References

[1] Alabdali, Ali A.; Byott, Nigel P. Counting Hopf–Galois structures on cyclic field extensions of squarefree degree. *J. Algebra* **493** (2018), 1–19. MR3715201, Zbl 06798687, arXiv:1703.09636, doi: 10.1016/j.jalgebra.2017.09.009. 1422

[2] Byott, Nigel P. Uniqueness of Hopf Galois structure of separable field extensions. *Comm. Algebra* **24** (1996), no. 10, 3217–3228. MR1402555, Zbl 0878.12001, doi: 10.1080/00927879608825743. 1422

[3] Byott, Nigel P. Hopf–Galois structures on field extensions with simple Galois groups. *Bull. London Math. Soc.* **36** (2004), no. 1, 23–29. MR2011974, Zbl 1038.12002, doi: 10.1112/S0024609303002595. 1422

[4] Caranti, Andrea; Dalla Volta, Francesca; Sala, Massimiliano. Abelian regular subgroups of the affine group and radical rings. *Publ. Math. Debrecen* **69** (2006), no. 3, 297–308. MR2273982, Zbl 1123.20002, arXiv:math/0510166. 1422, 1424, 1427

[5] Chase, Stephen U.; Sweedler, Moss E. Hopf algebras and Galois theory. Lecture Notes in Mathematics, 97. *Springer-Verlag, Berlin-New York*, 1969. ii+133 pp. MR0260724, Zbl 0197.01403, doi: 10.1007/BFb0101433. 1421

[6] Childs, Lindsay N. Elementary abelian Hopf Galois structures and polynomial formal groups. *J. Algebra* **283** (2005), no. 1, 292–316. MR2102084, Zbl 1071.16031, doi: 10.1016/j.jalgebra.2004.07.009. 1431, 1432

[7] Childs, Lindsay N. On Abelian Hopf Galois structures and finite commutative nilpotent rings. *New York J. Math.* **21** (2015), 205–229. MR3336553, Zbl 1318.13030. 1422, 1425

[8] Childs, Lindsay N. On the Galois correspondence for Hopf Galois structures. *New York J. Math.* **23** (2017), 1–10. MR3611070, Zbl 1396.12002, arXiv:1604.06066. 1434

[9] Childs, Lindsay N. Skew braces and the Galois correspondence for Hopf Galois structures. *J. Algebra* **511** (2018), 270–291. MR3834774, Zbl 1396.12003, arXiv:1802.03448, doi: 10.1016/j.jalgebra.2018.06.023. 1424, 1434

[10] Childs, Lindsay N. Bi-skew braces and Hopf Galois structures. *New York J. Math.* **25** (2019), 574–588. MR3982254, Zbl 07118581, arXiv:1904.08814. 1434

[11] Childs, Lindsay N.; Greither, Cornelius. Bounds on the number of ideals in finite commutative nilpotent $\mathbb{F}_p$-algebras. *Publ. Math. Debrecen* **92** (2018), no. 3–4, 495–516. MR3789700, Zbl 1399.13026, arXiv:1706.02518. 1434

[12] Featherstonhaugh, S. C.; Caranti, Andrea; Childs, Lindsay N. Abelian Hopf Galois structures on prime-power Galois field extensions. *Trans. Amer. Math. Soc.* **364** (2012), no. 7, 3675–3684. MR2901229, Zbl 1287.12002, doi: 10.1090/S0002-9947-2012-05503-6. 1422, 1425

[13] Greither, Cornelius; Pareigis, Bodo. Hopf Galois theory for separable field extensions. *J. Algebra* **106** (1987), no. 1, 239–258. MR0878476, Zbl 0615.12026, doi: 10.1016/0021-8693(87)90029-9. 1421, 1422

[14] Guarneri, L.; Vendramin, Leandro. Skew braces and the Yang–Baxter equation. *Math. Comp.* **86** (2017), no. 307, 2519–2534. MR3647970, Zbl 1371.16037, arXiv:1511.03171, doi: 10.1090/mcom/3161. 1422

[15] Rump, Wolfgang. Braces, radical rings, and the quantum Yang–Baxter equation. *J. Algebra* **307** (2007), no. 1, 153–170. MR2278047, Zbl 1115.16022, doi: 10.1016/j.jalgebra.2006.03.040. 1422, 1423

[16] Smoktunowicz, Agata; Vendramin, Leandro. On skew braces (with an appendix by N. Byott and L. Vendramin). *J. Comb. Algebra* **2** (2018), no. 1, 47–86. MR3763907, Zbl 06857320, arXiv:1705.06958, doi: 10.4171/JCA/2-1-3. 1422

[17] Wilson, Robert A. The finite simple groups. Graduate Texts in Mathematics, 251, *Springer-Verlag London, Ltd., London*, 2009. xvi+298 pp. ISBN: 978-1-84800-987-5. MR2562037 (2011e:20018), Zbl 1203.20012, doi: 10.1007/978-1-84800-988-2. 1426, 1429, 1430

(Lindsay Childs) Department of Mathematics and Statistics, University at Albany, Albany, NY 12222, USA
lchilds@albany.edu

This paper is available via http://nyjm.albany.edu/j/2019/25-58.html.