New York Journal of Mathematics

New York J. Math. **21** (2015) 205–229.

On Abelian Hopf Galois structures and finite commutative nilpotent rings

Lindsay N. Childs

Abstract. Let G be an elementary abelian p-group of rank n, with p an odd prime. In order to count the Hopf Galois structures of type G on a Galois extension of fields with Galois group G, we need to determine the orbits under conjugation by $\mathrm{Aut}(G)$ of regular subgroups of the holomorph of G that are isomorphic to G. The orbits correspond to isomorphism types of commutative nilpotent $\mathbb{F}_p$-algebras N of dimension n with $N^p = 0$. Adapting arguments of Kruse and Price, we obtain lower and upper bounds on the number $f_c(n)$ of isomorphism types of commutative nilpotent algebras N of dimension n (as vector spaces) over the field $\mathbb{F}_p$ satisfying $N^3 = 0$. For $n = 3$, 4 there are five, resp. eleven isomorphism types of commutative nilpotent algebras, independent of p (for $p > 3$). For $n \geq 6$, we show that $f_c(n)$ depends on p. In particular, for $n = 6$ we show that $f_c(n) \geq \lfloor (p-1)/6 \rfloor$ by adapting an argument of Suprunenko and Tyschkevich. For $n \geq 7$, $f_c(n) \geq p^{n-6}$. Conjecturally, $f_c(5)$ is finite and independent of p, but that case remains open. Finally, applying a result of Poonen, we observe that the number of Hopf Galois structures of type G is asymptotic to $f_c(n)$ as n goes to infinity.

Contents

Received February 7, 2015.

2010 *Mathematics Subject Classification.* Primary: 13E10, 12F10; Secondary: 20B35.

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

ISSN 1076-9803/2015

1. Introduction

Let L/K be a Galois extension with Galois group Γ of order m. If H is a cocommutative K-Hopf algebra and L is an H-module algebra, then L/K is an H-Hopf Galois extension of K if the obvious map

$$L \otimes_K H \to \mathrm{End}_K(L)$$

is a bijection. (The map is an isomorphism of K-algebras if one puts a cross product multiplication on the domain.) Greither and Pareigis [GP87] showed that if L/K is a H-Galois extension, then $L \otimes H \cong LN$ as Hopf algebras, where N is a regular subgroup of $\mathrm{Perm}(\Gamma)$ that is normalized by $\lambda(\Gamma)$, the image in $\mathrm{Perm}(\Gamma)$ of the left regular representation

$$\lambda : \Gamma \to \mathrm{Perm}(\Gamma), \quad \lambda(g)(x) = gx.$$

Here, a regular subgroup N of $\mathrm{Perm}(\Gamma)$ is a subgroup so that $|N| = |\Gamma|$ and $\{\eta(x) : \eta \in N\} = \Gamma$ for every x in Γ.

The correspondence given by base change from K to L and Galois descent from L to K then yields a bijection

$$\{\text{Hopf Galois structures on } L/K\}$$
$$\longleftrightarrow$$
$$\{\text{regular subgroups of } \mathrm{Perm}(\Gamma) \text{ normalized by } \lambda(\Gamma)\}.$$

Let $\mathcal{S}$ be a set of representatives of the isomorphism classes of groups of order n. If H is a K-Hopf algebra and $L \otimes_K H \cong LN$ where $N \cong G$ for some G in $\mathcal{S}$, we say that H has *type* G. Thus there is a bijection

$$\{\text{Hopf Galois structures on } L/K \text{ of type } G\}$$
$$\longleftrightarrow$$
$$\{\text{regular subgroups of } \mathrm{Perm}(\Gamma) \text{ normalized by } \lambda(\Gamma) \text{ and isomorphic to } G\}.$$

Rather than seeking Hopf Galois structures of type G by looking directly at regular subgroups of $\mathrm{Perm}(\Gamma)$ normalized by $\lambda(\Gamma)$ and isomorphic to G, an alternate approach is to work with the holomorph of G,

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

the normalizer of $\lambda(G)$ in $\mathrm{Perm}(G)$ (where ρ is the right regular representation of G in $\mathrm{Perm}(G)$). As shown in [By96], there is a bijection:

$$\{\text{regular subgroups of } \mathrm{Perm}(\Gamma) \text{ normalized by } \lambda(\Gamma) \text{ and isomorphic to } G\}$$
$$\longleftrightarrow$$
$$\{\text{equivalence classes of regular embeddings from } \Gamma \text{ to } \mathrm{Hol}(G)\}$$

where two embeddings β and $\beta' : \Gamma \to \mathrm{Hol}(G)$ are equivalent if there is an automorphism α of $\mathrm{Aut}(G) \subset \mathrm{Hol}(G)$ so that for all γ in Γ,

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

in $\mathrm{Perm}(G)$. We will work exclusively with the holomorph $\mathrm{Hol}(G)$ in this paper.

Call two regular subgroups J and J' of $\mathrm{Hol}(G)$ *conjugate* if there is an α in $\mathrm{Aut}(G)$ so that $J' = \alpha^{-1}J\alpha = C(\alpha)(J)$. If two regular embeddings β and β' are equivalent, then $\beta(\Gamma)$ and $\beta'(\Gamma)$ are conjugate. Conversely, if J and J' are conjugate, $J' = \alpha^{-1}J\alpha$, and $\beta : \Gamma \to J$ is a regular embedding, then $\beta' : \Gamma \to J'$ given by $\beta'(\gamma) = \alpha^{-1}\beta(\gamma)\alpha = C(\alpha)\beta$ is equivalent to β. So to find equivalence classes of regular embeddings of Γ to $\mathrm{Hol}(G)$, we may partition the set of regular subgroups of $\mathrm{Hol}(G)$ isomorphic to Γ into orbits, conjugacy classes under the action of $\mathrm{Aut}(G)$, pick a representative J of each orbit, and determine the regular embeddings of Γ into J.

Let $\mathrm{Sta}(J)$ be the subgroup of elements $C(\alpha)$ in $\mathrm{Aut}(J)$ for α in $\mathrm{Aut}(G)$, such that $C(\alpha)(J) := \alpha^{-1}J\alpha = J$.

Proposition 1.1. *For J a representative of a conjugacy class of regular subgroups of $\mathrm{Hol}(G)$ isomorphic to Γ, the number of equivalence classes of embeddings of Γ into $\mathrm{Hol}(G)$ with image J is equal to $|\mathrm{Aut}(\Gamma)|/|\mathrm{Sta}(J)|$.*

Proof. If $\beta : \Gamma \to \mathrm{Hol}(G)$ is a regular embedding with image J, then so is $\beta\theta$ for any automorphism θ of Γ. If $\beta' : \Gamma \to \mathrm{Hol}(G)$ is a regular embedding with image J and is equivalent to β, then $\beta' = C(\alpha)\beta$ for some α in $\mathrm{Sta}(J)$. But then $\beta^{-1}\beta' = \beta^{-1}C(\alpha)\beta = \theta$ is an automorphism of Γ, and $C(\alpha)\beta = \beta\theta$. So we have an embedding of $\mathrm{Sta}(J)$ into $\mathrm{Aut}(\Gamma)$ by $C(\alpha) \mapsto \theta$, and two regular embeddings $\beta, \beta\theta$ are equivalent iff θ is in the image in $\mathrm{Aut}(G)$ of $\mathrm{Sta}(J)$. □

Since the stabilizers of different subgroups in the orbit of J are isomorphic, the number in Proposition 1.1 is independent of the choice of J in an orbit of regular subgroups of $\mathrm{Hol}(G)$.

This count then yields:

Theorem 1.2. *The number of Hopf Galois structures of type G on a Galois extension L/K with Galois group Γ is equal to*

$$\sum_{J \in \mathcal{C}} |\mathrm{Aut}(\Gamma)|/|\mathrm{Sta}(J)|$$

where $\mathcal{C}$ is a set of representatives of all orbits (conjugacy classes) in $\mathrm{Hol}(G)$ of regular subgroups isomorphic to Γ.

This result implies that the number of orbits in $\mathrm{Hol}(G)$ plays a key role in the count of Hopf Galois structures. We focus on that number in this paper.

In this paper G is an elementary abelian p-group of rank n, and the Galois group Γ of L/K is isomorphic to G. Assume $p \geq 3$ throughout.

The main point of the paper is to utilize the result of Caranti, Della Volta and Sala [CDVS06] that gives a bijection between orbits of regular subgroups of $\mathrm{Hol}(G)$ and isomorphism types of commutative nilpotent $\mathbb{F}_p$-algebra structures on the additive group G. That correspondence transforms

the problem of counting orbits into that of counting isomorphism types of commutative nilpotent $\mathbb{F}_p$-algebras.

The corresponding problem over an algebraically closed field instead of over $\mathbb{F}_p$ has been studied by several researchers during the past half-century, for example, Suprunenko and Tyshkevich [ST68], and more recently by Poonen [Po08b]. The main result is that for $n \leq 5$, there is a finite number of isomorphism types of commutative nilpotent algebras, while for $n \geq 6$ there is an infinite number. These authors have primarily focused on counting commutative nilpotent algebras N with $N^3 = 0$, a class that is particularly convenient for us because such algebras correspond to regular subgroups isomorphic to G, and hence to Hopf Galois structures of type G on a Galois extension with Galois group G.

The problem of bounding the number of isomorphism types of nilpotent algebras over a finite field was studied by Kruse and Price [KP69] and more recently, by de Graaf [deG10] for nilpotent algebras of dimensions 3 and 4. Poonen [Po08a] has studied a related problem. We will note Poonen's work in the final section of this paper.

By analogy with nilpotent algebras of finite dimension over an algebraically closed field (cf. Poonen [Po08b]), a natural conjecture is that for $n \leq 5$, the number of isomorphism types of commutative nilpotent $\mathbb{F}_p$-algebras is a finite number bounded by a constant independent of p, while for $n \geq 6$ the number of isomorphism types is a function that goes to infinity with p.

As we shall show, the conjecture is known except for $n = 5$.

In the final section, we show that the number of Hopf Galois structures of type $G = \mathbb{F}_p^n$ on a Galois extension L/K with Galois group G is asymptotic to $p^{(2n^3)/27}$ as $n \mapsto \infty$.

This paper is a sequel to but is independent of [Ch05]. It began as notes for a talk at the 2014 Omaha workshop, Ramification and Galois Module Theory. My special thanks to Griff Elder for his inspiration and enthusiasm, and to him and the University of Nebraska at Omaha for their warm hospitality each of the last three years. My thanks to the referee for a careful reading of the manuscript and, in particular, for pointing out an error in an earlier version of Proposition 4.1.

For the remainder of the paper, p is an odd prime and $G \cong (\mathbb{F}_p^n, +)$, an elementary abelian p-group of rank n. We are ultimately interested in the number $t_n(G)$ of Hopf Galois structures of type G on a Galois field extension L/K with Galois group $\Gamma \cong G$.

2. Nilpotent ring structures associated to abelian regular subgroups

For $G = (\mathbb{F}_p^n, +)$, we wish to study isomorphism types of regular subgroups of $\mathrm{Hol}(G)$. Recall that a regular subgroup J of $\mathrm{Perm}(G)$ is a subgroup of

$\mathrm{Perm}(G)$ so that $|J| = |G|$ and $\{\eta(e) \mid \eta \in J\} = G$, where e is the identity element of G.

In this section we associate a commutative nilpotent $\mathbb{F}_p$-algebra to a regular subgroup, following [CDVS06]. Here is how it is done.

Let J be an abelian regular subgroup of $\mathrm{Hol}(G)$, where $G = (\mathbb{F}_p^n, +)$. Then associated to J is a function (not a homomorphism)

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

where for x in G, $\tau(x)$ is the unique element

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

of J whose last column is $(x, 1)^T$.

Let $\delta(x) = A_x$. Define a multiplication on $(G, +)$ by

$$x \cdot y = \delta(x)(y) = A_x y.$$

Then, as Caranti, et. al. observe [CDVS06], this multiplication makes

$$N = (G, +, \cdot)$$

into a commutative nilpotent ring. Then the circle multiplication on N defined by

$$\begin{aligned} x \circ y &= x + y + x \cdot y \\ &= x + y + \delta(x)y \\ &= x + y + A_x y \end{aligned}$$

for all x, y in G defines a group structure on the set $\mathbb{F}_p^n$ so that $(\mathbb{F}_p^n, \circ) \cong J$ by the map

$$x \mapsto \begin{pmatrix} I + A_x & x \\ 0 & 1 \end{pmatrix}.$$

As shown in [CDVS06], the maps $J \mapsto (\mathbb{F}_p^n, +, \cdot)$ and $(\mathbb{F}_p^n, +, \cdot) \mapsto (\mathbb{F}_p^n, \circ)$ define a bijection between abelian regular subgroups of $\mathrm{Aff}(\mathbb{F}_p^n)$ and commutative nilpotent $\mathbb{F}_p$-algebras of $\mathbb{F}_p$-dimension n.

Conjugacy of two regular subgroups in $\mathrm{Hol}(C_p^n)$ translates nicely, as shown in [CDVS06]:

Proposition 2.1. *Two commutative nilpotent $\mathbb{F}_p$-algebras are isomorphic iff the corresponding abelian regular subgroups of $\mathrm{Hol}(G) = \mathrm{Aff}(\mathbb{F}_p^n)$ are in the same orbit under conjugation by elements of $\mathrm{Aut}(G) = \mathrm{GL}_n(\mathbb{F}_p)$.*

Thus the problem of determining the number of orbits for $G = (\mathbb{F}_p^n, +)$ becomes one of determining the number of isomorphism types of commutative nilpotent $\mathbb{F}_p$-algebras of dimension n. In particular, estimating the number of orbits in $\mathrm{Hol}(G)$ of regular subgroups isomorphic to $G = (\mathbb{F}_p^n, +)$, translates by Proposition 2.1 to estimating the number of isomorphism types of commutative nilpotent $\mathbb{F}_p$-algebras of $\mathbb{F}_p$-dimension n whose corresponding circle group is isomorphic to G.

It turns out that many regular subgroups of $\mathrm{Hol}(G)$ are isomorphic to G. To support that statement, we cite two results. The first is a lemma of Caranti:

Proposition 2.2. *Let $p \geq 3$ and let $G = (\mathbb{F}_p^n, +)$. If N is a commutative nilpotent $\mathbb{F}_p$-algebra of dimension n with $N^p = 0$, then the regular subgroup of $\mathrm{Hol}(G)$ defined by the circle operation on N is isomorphic to G.*

Proof. Let N be is a commutative nilpotent $\mathbb{F}_p$-algebra of dimension n with $N^p = 0$. Then the circle operation on N defined by $a \circ b = a + b + a \cdot b$ makes $(\mathbb{F}_p^n, \circ)$ into the corresponding regular subgroup of $\mathrm{Hol}(G)$. Let

$$m_\circ a = a \circ a \circ \cdots \circ a \ (m \text{ factors }).$$

Then [FCC12, Lemma 3] shows that for a in N,

$$p_\circ a = pa + \sum_{i=2}^{p-1} \binom{p}{i} a^i + a^p,$$

and therefore $p \circ a = a^p$. Since $a^p = 0$, we have $p_\circ a = 0$ for all a in $(\mathbb{F}_p^n, \circ)$. Hence $(\mathbb{F}_p^n, \circ)$ is isomorphic to G. □

As a consequence, we have

Theorem 2.3. *Let $p \geq 3$ and $G = (\mathbb{F}_p^n, +)$ The number of $\mathrm{Aut}(G)$-orbits of regular subgroups J of $\mathrm{Hol}(G)$ with $J \cong G$ is bounded from below by the number of isomorphism classes of commutative $\mathbb{F}_p$-algebras N of dimension n with $N^3 = 0$.*

The other result buttressing the claim that many regular subgroups of $\mathrm{Hol}(G)$ are isomorphic to G is Featherstonhaugh's Theorem [Fe03]. As sharpened in [FCC12], it is

Theorem 2.4. *Let $G \cong (\mathbb{F}_p^n, +)$. If $p > n$, then every abelian regular subgroup of $\mathrm{Hol}(G)$ is isomorphic to G.*

3. An upper bound

We observed in Section 2 that the number of orbits of regular subgroups of $\mathrm{Aff}(\mathbb{F}_p^n)$ under the action of $\mathrm{Aut}(G) = \mathrm{GL}_n(\mathbb{F}_p)$ is equal to the number of isomorphism types of commutative nilpotent ring structures on $(\mathbb{F}_p^n, +, \cdot)$ on the additive group $G = (\mathbb{F}_p^n, +)$. Among those nilpotent rings N, those with $N^3 = 0$ are of particular interest because, by Caranti's Lemma, they yield regular subgroups of $\mathrm{Hol}(G)$ that are isomorphic to G.

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

In this section, we obtain an upper bound for $f_c(n, r)$, adapting an argument of Kruse and Price [KP70].

Theorem 3.1. *Let $f_c(n,r)$ be the number of pairwise nonisomorphic commutative $\mathbb{F}_p$-algebras N with $\dim_{\mathbb{F}_p} N = n, \dim_{\mathbb{F}_p}(N/N^2) = r$, and $N^3 = 0$. Then*

$$f_c(n,r) \leq p^{\binom{r^2+r}{2}(n-r)-(n-r)^2+(n-r)}$$

Proof. Let R be the free commutative $\mathbb{F}_p$-algebra with generators $x_1, \ldots, x_r$. Then R may be viewed as the ideal generated by $x_1, \ldots, x_r$ in the polynomial ring $R = \mathbb{F}_p[x_1, \ldots, x_r]$. Let $F = R/R^3$. Let N be a commutative nilpotent $\mathbb{F}_p$-algebra of F_p-dimension n with $N^3 = 0$, and let $\dim(N/N^2) = r$. Mapping F onto N by sending the image of $x_1, \ldots, x_r$ in F to elements of N whose images modulo N^2 is an $\mathbb{F}_p$-basis of N/N^2 is a surjective $\mathbb{F}_p$-algebra homomorphism with kernel I. The ideal I determines N up to isomorphism: $N \cong F/I$ where $I \subset F^2$. Then $I^2 = 0$, so the ideal I may simply be viewed as an $\mathbb{F}_p$-subspace of F^2.

Now

$$\dim(F^2) = r^2 - \binom{r}{2} = \frac{(r^2+r)}{2},$$

the number of distinct monomials of degree 2 in R. That number is equal to the number of ordered pairs (i,j) for $1 \leq i,j \leq r$ minus the number of pairs (i,j) for $i \neq j$ (since $x_i x_j = x_j x_i$ for N commutative). Under the map from $F \to N$, the kernel $I \subset F^2$ and F^2 maps onto N^2. Hence $\dim(N^2) + \dim(I) = \dim(F^2)$, and so

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

This last computation implies that $n - r \leq \frac{r^2+r}{2}$.

Thus the number $f_c(n,r)$ of commutative nilpotent algebras N of dimension n with $\dim(N/N^2) = r$ and $N^3 = 0$ satisfies

$$\begin{aligned} f_c(n,r) \leq\ & \#\text{ of ideals } I \text{ of } F^2 \text{ of dimension } \frac{(r^2+r)}{2} - (n-r), \\ =\ & \#\text{ of subspaces } I \text{ of } F^2 \text{ of dimension } \frac{(r^2+r)}{2} - (n-r). \end{aligned}$$

Since F^2 is a space of dimension $s = (r^2+r)/2$, the number of subspaces of F^2 of dimension $s-(n-r)$ is equal to the number of subspaces of dimension $n-r$. (View one collection of subspaces as row spaces of matrices and the other collection as the corresponding null spaces.)

To determine the number of subspaces of F^2 of dimension $n-r$, pick sets of $n-r$ linearly independent elements of F^2 sequentially: there are $p^s - 1$ choices for the first element, then $p^s - p$ choices for the second, etc., and $p^s - p^{n-r-1}$ choices for the $n-r$-th linearly independent element. These $n-r$ linearly independent elements define a subspace of dimension $n-r$. Any other basis of the same space can be transformed to the original basis by an element of $\mathrm{GL}_{n-r}(\mathbb{F}_p)$. So the number of subspaces of F^2 of dimension

$n-r$ is

$$\frac{(p^s-1)(p^s-p)\cdots(p^s-p^{n-r-1})}{(p^{n-r}-1)(p^{n-r}-p)\cdots(p^{n-r}-p^{n-r-1})}.$$

To get a convenient upper bound for $f_c(n,r)$, observe that

$$\frac{p^s-p^l}{p^k-p^l} < \frac{p^s}{p^{k-1}}$$

for all $0 \le l < k$, so we conclude that

$$f_c(n,r) \le p^a$$

where

$$\begin{aligned} a &= s(n-r) - (n-r-1)(n-r) \\ &= \left(\frac{r^2+r}{2}\right)(n-r) - (n-r)(n-r-1) \\ &= \left(\frac{r^2+r}{2}\right)(n-r) - (n-r)^2 + (n-r). \end{aligned}$$ □

This upper bound overstates the number of isomorphism classes of nilpotent algebras N of dimension n with $\dim(N/N^2) = r$, because the analysis does not account for changing algebra generators of a given nilpotent algebra. We can see this when we do the case $n = 3$, below, and also when $r = n-1$, which we consider in the next section.

4. When N^2 has dimension 1

The upper bound of Theorem 3.1 for isomorphism types of commutative nilpotent algebras N of dimension n with $N^3 = 0$ and $\dim N^2 = 1$ (hence $n - r = 1$) is

$$f_c(n,r) \le p^{\left(\frac{(n-1)^2+(n-1)}{2}\right)} = p^{\frac{n(n-1)}{2}}.$$

In this section we prove:

Proposition 4.1. *For $p > 3$ and $n \ge 3$ the number of isomorphism classes of commutative nilpotent algebras of dimension n with $\dim(N^2) = 1$ is $\frac{3n-3}{2}$ if n is odd, and $\frac{3n-4}{2}$ if n is even.*

Proof. Suppose N is a commutative nilpotent $\mathbb{F}_p$-algebra of dimension n, $N^3 = 0$ and $\dim(N^2) = 1$. Let N/N^2 have basis $x_1, \ldots, x_{n-1}$, let $\overline{x}^T = (x_1, \ldots, x_{n-1})$, and let N^2 have basis y. Define the $r \times r$ structure matrix $\Phi = (\phi_{ij})$ by

$$x_i x_j = \phi_{ij} y \quad \text{for} \quad i,j = 1, \ldots, n,$$

or more compactly,

$$\overline{x}\overline{x}^T = y\Phi.$$

Now N is commutative, so Φ is symmetric. Thus Φ is congruent by an invertible but not necessarily orthogonal matrix P (cf. [BW66], [Ka69] or

[BM53], IX, 8) to a unique diagonal matrix of a special form. More precisely, there is an invertible matrix P so that

$$P\Phi P^T = D = \operatorname{diag}(1, \dots, 1, d, 0, \dots, 0)$$

is diagonal and $d = 1$ or any nonsquare s. (Replacing x_k by bx_k for any b in $\mathbb{F}_p$ will replace s by $b^2 s$, thus we can choose the nonsquare s as we wish.) The number of zeros and the class of d modulo the subgroup of nonzero squares in $\mathbb{F}_p$ uniquely determines the class of Φ under congruence. Let $P\overline{x} = \overline{z}$ with $\overline{z}^T = (z_1, z_2, \dots, z_{n-1})$. Then N is isomorphic to $N_{k,d} = \langle z_1, z_2, \dots, z_{n-1} \rangle$ with

$$z_1^2 = \cdots = z_{k-1}^2 = y,\ z_k^2 = dy,\ z_{k+1}^2 = \cdots = z_{n-1}^2 = 0,\ z_i z_j = 0 \text{ for } i \neq j.$$

Thus the structure matrix for $N_{k,d}$ is

$$D_{k,d} = \operatorname{diag}(d_1, d_2, \dots, d_{n-1})$$

with $d_1 = \cdots = d_{k-1} = 1$, $d_k = d$, $d_{k+1} = \cdots = d_{n-1} = 0$.

Any invertible linear change of variables $Q\overline{z} = \overline{x}$, $w = sy$ will yield a nilpotent algebra N' isomorphic to N, where Φ is transformed to $sQ\Phi Q^T$. Since Q is invertible, the rank of Φ is preserved. Thus algebras corresponding to Φ of different ranks are not isomorphic.

Suppose k is odd. Since every nonzero element of $\mathbb{F}_p$ is a sum of two squares , we may write the nonsquare s as $s = f^2 + g^2$ for some f, g in $\mathbb{F}_p$. Let P_0 be the 2×2 matrix

$$P_0 = \begin{pmatrix} f & g \\ -g & f \end{pmatrix},$$

an invertible matrix since $\det(P) = s$. Then $P_0 P_0^T = \operatorname{diag}(s, s)$. Let Q be the $n-1 \times n-1$ block diagonal matrix

$$Q = \operatorname{diag}(P_0, P_0, \dots, P_0, s, 1, 1, \dots, 1)$$

with $(k-1)/2$ copies of P_0 along the diagonal. Then

$$QD_{k,1}Q^T = \operatorname{diag}(s, s, \dots, s^2, 0, 0, \dots, 0).$$

Let $\overline{z} = Q\overline{x}$ and $w = sy$. Then

$$\begin{aligned} \overline{z}\overline{z}^T &= Q\overline{x}\overline{x}^T Q^T \\ &= QD_{k,1}Q^T \\ &= y \operatorname{diag}(s, s, \dots, s^2, 0, 0, \dots, 0) \\ &= w \operatorname{diag}(1, 1, \dots, s, 0, 0, \dots, 0) \\ &= wD_{k,s}. \end{aligned}$$

Thus $N_{k,1} \cong N_{k,s}$.

Now suppose k is even. Suppose $N_{k,1}$ has basis $x_1, \dots, x_{n-1}, y$ as above with $n-1 \times n-1$ structure matrix $D_1 = \operatorname{diag}(1, 1, \dots, 1, 0, \dots, 0)$ (k 1's). Then

$$\overline{x}\overline{x}^T = yD_1.$$

Similarly, suppose $N_{k,s}$ has basis $z_1, \dots, z_{n-1}, w$ with structure matrix

$$D_s = \operatorname{diag}(1, 1, \dots, 1, s, 0, \dots, 0)$$

(with $k-1$ 1's). Then

$$\overline{z}\overline{z}^T = wD_s.$$

Now $N_{k,1}$ is isomorphic to $N_{k,s}$ if and only if there is an invertible $(n-1) \times (n-1)$ matrix P and a nonzero element b of $\mathbb{F}_p$ so that

$$\overline{z} = P\overline{x} \quad \text{and} \quad w = by.$$

Substituting, P and b must satisfy

$$PD_1P^T = bD_s.$$

Write

$$P = \begin{pmatrix} P_{11} & P_{12} \\ P_{21} & P_{22} \end{pmatrix}$$

where P_{11} is $k \times k$. Then we must have

$$P_{11}P_{11}^T = b \operatorname{diag}(1, \dots, 1, s).$$

Then

$$\det(P_{11}^2) = b^k s.$$

Since k is even, this would imply that s is a square. Hence the n-dimensional algebras $N_{k,1}$ and $N_{k,s}$ cannot be isomorphic when s is a nonsquare in $\mathbb{F}_p$ and k is even.

The number of isomorphism types of commutative nilpotent algebras N of dimension n with $\dim N^2 = 1$ is then

$$1, 3, 4, 6, 7, 9, \dots, \quad \text{for} \quad n-1 = 1, 2, 3, 4, 5, 6, \dots.$$

The count in the statement of the theorem is easily obtained. □

The case $n = 3$. There are five isomorphism types of commutative nilpotent algebras of dimension 3. Let N be a nilpotent algebra of dimension $n = 3$ over $\mathbb{F}_p$. If $N^3 = 0$ and $\dim(N/N^2) = r$, then $\dim(N^2) = 3 - r$, so r cannot be $= 1$. If $r = 3$ then $N^2 = 0$. If $r = 2$ then $\dim(N^2) = 1$, the case just covered: we obtain $N_{1,1}, N_{2,1}$ and $N_{2,s}$ for s a nonsquare in $\mathbb{F}_p$. The only other isomorphism type of dimension 3 has $r = 1$, in which case $N = \langle x \rangle$ with $x^4 = 0$.

In [Ch05] we determined the number of orbits of regular subgroups in $\operatorname{Hol}(G)$ under conjugation for $n \leq 3$ by associating to a regular subgroup a commutative nilpotent polynomial degree 2 formal group, and then using the fact that conjugate regular subgroups correspond to linearly isomorphic formal groups. Using that correspondence, [Ch05] showed that for $n = 1, 2, 3$ there are $1, 2, 5$ orbits, resp. For $n = 3$ there is one orbit with $r = 3$, three orbits with $r = 2$ and one with $r = 1$. The approach here, using nilpotent ring structures and the methods of this section, is more efficient.

5. When I has dimension 1

We can also apply the diagonalization when $\dim(I) = 1$. This case occurs when

$$1 = \dim(I) = \dim(R^2) - \dim(N^2) = \frac{r^2 + r}{2} - (n - r) = \frac{r^2 + 3r}{2} - n.$$

The possibilities include $(n, r) = (2, 1), (4, 2), (8, 3), (13, 4), (19, 5), (26, 6)$, etc. Then $I = \langle q \rangle$, a quadratic form in r variables, where, after a linear change of generators of R as before, we may assume that q has the form

$$q = x_1^2 + \cdots + x_{k-1}^2 + dx_k^2$$

with $d = 1$ or $d = s'$. Since the ideal I uniquely determines the algebra N, the number of classes of commutative nilpotent algebras of dimension n with I principal is equal to $2r - 1$.

6. The case $n = 4$

There are eleven isomorphism types of commutative nilpotent $\mathbb{F}_p$-algebras N of dimension $n = 4$.

We first look at the case where $N^3 = 0$.

Let N be a commutative $\mathbb{F}_p$-algebra of dimension n . Let $r = \dim(N/N^2)$. If $r = 4$ then $N^2 = 0$. If $r = 1$ then $N = \langle x \rangle$ with $x^5 = 0$. So the cases of interest are $r = 2$ and $r = 3$.

Assume $N^3 = 0$.

If $r = \dim(N/N^2) = 3$, then $\dim(N^2) = 1$, so by Proposition 4.1 there are four isomorphism types of commutative nilpotent $\mathbb{F}_p$-algebras N of dimension 4, when $\dim(N^2) = 1$.

If $r = \dim(N/N^2) = 2$, then $\dim(N^2) = 2$, while $\dim(R^2) = 3$, so $\dim(I) = 1$. Thus I is a principal ideal of R, generated by a quadratic form in two variables. The ideal doesn't change under congruence of the corresponding symmetric matrix. So there are three possible ideals, corresponding to the the vectors of coefficients of the quadratic forms that represent the congruence classes under congruence:

$$(1, 0)$$
$$(1, 1)$$
$$(1, s')$$

where s' is a nonsquare in $\mathbb{F}_p$. Including the case where $N^2 = 0$, we have:

Proposition 6.1. *For $n = \dim(N) = 4$, there are exactly eight isomorphism classes of commutative nilpotent $\mathbb{F}_p$-algebras N with $N^3 = 0$.*

This compares with the upper bound of Theorem 3.1, which involves powers of p:

For $n = 4, r = 2$ the upper bound $f_c(4, 2) \leq (p^3 - 1)/(p - 1) = p^2 + p + 1$.

For $n = 4, r = 3$ the upper bound

$$f_c(4,3) \leq (p^6 - 1)/(p-1) = p^5 + p^4 + p^3 + p^2 + p + 1.$$

If $n = 4$ and $N^3 \neq 0$ there are three isomorphism types. One of them has $r = \dim(N/N^2) = 1$: then $N = \langle x \rangle$ with $x^5 = 0$: the Jordan block example of [Ch05]. The remaining two have $\dim(N/N^2) = 2, \dim(N^2/N^3) = 1$ and $\dim(N^3) = 1$. We omit this case here. The argument in subsection 1.1 of [Po08b] may be adapted to $\mathbb{F}_p$ to show that there are two isomorphism types; also, the full classification of commutative nilpotent algebras of dimensions 3 and 4 has been obtained by Willem de Graaf [deG10].

7. The case $n = 5$

We briefly consider commutative nilpotent $\mathbb{F}_p$-algebras of dimension 5 with $N^3 = 0$.

Recall $r = \dim N/N^2$. Thus $r = 1$ is not possible.

If $r = 2$, then we must have $\dim(N^2) = 3$, which implies that $\dim(N^2) = \dim(R^2)$, so $I = 0$, and $N \cong R/R^3$.

If $r = 4$, then $\dim(N^2) = 1$, so Proposition 4.1 applies with $n = 5$ to give six isomorphism classes of commutative nilpotent algebras with $N^3 = 0$: the vector of diagonal entries of the structure matrix Φ can be

$$(1,0,0,0), (1,1,0,0), (1,s',0,0), (1,1,1,0), (1,1,1,1), (1,1,1,s')$$

where s' is a fixed nonsquare in $\mathbb{F}_p$.

Thus the remaining interesting case is $r = 3$. Then $\dim(N^2) = 2$, $\dim(R^2) = 6$ and $\dim(I) = 4$. This is the most complicated case in [Po08b]. Both Poonen [Po08b] and Suprunenko and Tyshkevich ([ST68], Theorem 18) obtain a total of thirteen isomorphism types of commutative nilpotent algebras N of dimension 5 with $N^3 = 0$ over an algebraically closed field. Of those, one has $r = 2$ and four have $r = 4$. (The six over $\mathbb{F}_p$ with $r = 4$ reduce to four because there is no nonsquare over an algebraically closed field.) The argument in [ST68] utilizes a normal form for a complex symmetric matrix under action by the orthogonal group, a result that apparently has no counterpart over a finite field.

8. A lower bound

We found in Section 3 an upper bound for $f_c(n,r)$, the number of pairwise nonisomorphic commutative $\mathbb{F}_p$-algebras N with

$$\dim_{\mathbb{F}_p} N = n, \quad \dim_{\mathbb{F}_p}(N/N^2) = r, \quad \text{and} \quad N^3 = 0.$$

We now seek a lower bound on $f_c(n,r)$. As with the upper bound, we adapt an argument of Kruse and Price [KP70], [KP69]. The method generalizes the argument in the proof of Proposition 4.1.

Theorem 8.1. *Let $f_c(n,r)$ be as just defined. Then*

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

Proof. Let N be a commutative nilpotent $\mathbb{F}_p$-algebra of dimension n, where $\dim(N/N^2 = r$, $\dim(N^2) = n-r$ and $N^3 = 0$. Let μ_a be the multiplication on N:

$$\mu_N : N \times N \to N.$$

Then μ_N maps onto N^2, and for every a in N^2, $\mu_N(ab) = 0$ for all b in N since $N^3 = 0$. So μ uniquely defines and is defined by a map

$$\overline{\mu} : N/N^2 \times N/N^2 \to N^2.$$

Let N have an $\mathbb{F}_p$-basis $\{e_1, \ldots, e_r, f_1, \ldots, f_{n-r}\}$ where the first r elements define modulo N^2 a basis of N/N^2. The ring structure on N is defined by $n-r$ matrices $\Phi^{(k)} = (\phi_{ij}^{(k)})$ of structure constants $\phi_{ij}^{(k)}$ defined by

$$e_i e_j = \sum_{k=1}^{n-r} \phi_{ij}^{(k)} f_k.$$

If we let $\overline{e}_1, \ldots, \overline{e}_r$ be the induced basis of N/N^2, then the structure constants only depend on $\{\overline{e}_1, \ldots, \overline{e}_r\}$ and $\{f_1, \ldots, f_{n-r}\}$. Since N is commutative, $\phi_{ij}^{(k)} = \phi_{ji}^{(k)}$, that is, the $\Phi^{(k)}$ are symmetric matrices in $\mathrm{M}_r(\mathbb{F}_p)$. There are no conditions on the ϕ related to associativity because $N^3 = 0$. So each choice of the symmetric structure matrices $\{\Phi^{(k)} \mid k = 1, \ldots, n-r\}$ will define a commutative nilpotent algebra structure.

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

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

We may view a nilpotent $\mathbb{F}_p$-algebra N with $\dim(N) = n$ and $\dim(N^2) = n-r$ as uniquely corresponding to a multiplication map

$$\mu_N : \mathbb{F}_p^r \times \mathbb{F}_p^r \to \mathbb{F}_p^{n-r} :$$

we fix a basis $(e_1, \ldots, e_r)$ for $\mathbb{F}_p^r$, a basis $(f_1, \ldots, f_{n-r})$ for $\mathbb{F}_p^{n-r}$, and a set $\{\Phi^{(1)}, \ldots, \Phi^{(n-r)}\}$ of structure constants, and define a multiplication μ_N by the structure constants:

$$\mu_N(e_i, e_j) = e_i \cdot e_j = \sum_{k=1}^{n-r} \phi_{ij}^{(k)} f_k,$$

where $\Phi^{(k)} = (\phi_{ij}^{(k)})$.

Let $Q \in \mathrm{GL}_{n-r}(\mathbb{F}_p)$ and $P \in \mathrm{GL}_r(\mathbb{F}_p)$. Let $Q^{-1} = (q_{ij})$. Define new bases of $\mathbb{F}_p^r$ and $\mathbb{F}_p^{n-r}$ by

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_r \end{pmatrix} = P \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_r \end{pmatrix}, \quad Q \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_{n-r} \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_{n-r} \end{pmatrix}.$$

Then

$$\begin{aligned} a_i \cdot a_j &= \sum_{k=1}^{r} p_{ik} e_k \cdot \sum_{l=1}^{r} p_{jl} e_l \\ &= \sum_{k,l=1}^{r} p_{ik} \phi_{kl}^{(m)} p_{jl} \sum_{\nu=1}^{n-r} q_{m\nu} b_\nu \\ &= \sum_{\nu} \theta_{ij}^{(\nu)} b_\nu. \end{aligned}$$

So

$$\theta_{ij}^{(\nu)} = \sum_{k,l=1}^{r} p_{ik} \phi_{kl}^{(m)} p_{jl} q_{m\nu},$$

where $\Theta^{(\nu)} = (\theta_{ij}^{(\nu)})$. We have

$$\Theta^{(\nu)} = \sum_{m=1}^{n-r} q_{m\nu} P \Phi^{(m)} P^T.$$

Composition works: acting by (P, Q), then by (R, S) is the same as acting by (RP, SQ).

Thus the group $H = \mathrm{GL}_{n-r}(\mathbb{F}_p) \times \mathrm{GL}_r(\mathbb{F}_p)$ acts on the set $\mathcal{S}$ of sets of structure constants, and two sets of structure constants in the same orbit under the action of H define isomorphic $\mathbb{F}_p$-algebras. Conversely, if two $\mathbb{F}_p$-algebras are isomorphic, then there is an element of H that maps one to the other, so the corresponding sets of structure constants are in the same orbit under H.

Therefore, the number $f_c(n, r)$ of isomorphism classes of commutative nilpotent $\mathbb{F}_p$-algebras N with $\dim(N) = n, \dim(N^2) = n - r$ and $N^3 = 0$ satisfies

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

So

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

Hence

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

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

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

where

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

Note that the exponent b of p in the lower bound is in fact less than the upper bound a found in Section 3: $a = b + (n - r + r^2)$.

Since $f_c(n,r)$ counts the number of isomorphism types of nilpotent algebras N with $\dim(N/N^2) = r$, $\dim(N^2) = n - r$ and $N^3 = 0$, it is a lower bound on $t_n(G)$, the number of Hopf Galois structures of type G on a Galois extension L/K with Galois group G.

The lower bound on $f_c(n,r)$ just found goes to infinity with n when r is near $2n/3$. In fact, for $r = 2n/3$,

$$b = \frac{2n^2}{27}(n-6).$$

More precisely:

Proposition 8.2. *For $n \geq 7$, there is an r so that $f_c(n,r)$ is bounded from below by p^b where b is positive. Hence $t_n(G)$ is bounded from below by a positive power of p for $n \geq 7$.*

Proof. Let $n = 3m + s$ with $s = 0, 1, 2$. Let $r = 2m$ and $n - r = m + s$. Then

$$\begin{aligned} b &= \frac{(2m)^2 + 2m)}{2}(m+s) - (m+s)^2 - (2m)^2 \\ &= 2m^3 - (4-2s)m^2 - ms - s^2. \end{aligned}$$

For $s = 0$, $b = 2m^3 - 4m^2 > 0$ for $m \geq 3$;
For $s = 1$, $b = 2m^3 - 2m^2 - m - 1 > 0$ for $m \geq 2$;
For $s = 2$, $b = 2m^3 - 2m - 4 > 0$ for $m \geq 2$.
So $f_c(m,r) = f_c(3m+s, 2m) > p^b$ and $b > 0$ for all $n \geq 7$. $\square$

For $r = n - 2$ we get a clean lower bound:

Corollary 8.3.

$$\begin{aligned} f_c(n, n-2) &\geq \frac{p^{\left(\frac{(n-2)^2+(n-2)}{2}\right)^2}}{p^{(n-2)^2}p^4} \\ &= \frac{p^{(n-2)^2}p^{n-2}}{p^{(n-2)^2}p^4} = p^{n-6}. \end{aligned}$$

However, for $n \leq 6$ the lower bound is not informative.

For $n \leq 5$ the exponent of p on the bound

$$f_c(n,r) \geq p^{\frac{1}{2}(r^2(n-r)+r(n-r)-2(n-r)^2-2r^2)}$$

is negative for all r, hence gives no information on the possible number of commutative nilpotent $\mathbb{F}_p$ algebras of dimension 5.

9. The case $n = 6$

The lower bound on $f_c(n,r)$ is also not helpful for $n = 6$.

For $n = 6, r = 4$, the more precise lower bound,

$$f_c(n,r) \geq \frac{p^{(\frac{r^2+r}{2})(n-r)}}{|\mathrm{GL}_{n-r}(\mathbb{F}_p)| \cdot |\mathrm{GL}_r(\mathbb{F}_p)|}$$

is

$$f_c(6,4) \geq \frac{1}{(\frac{p-1}{p})^2(\frac{p^2-1}{p^2})^2(\frac{p^3-1}{p^3})(\frac{p^4-1}{p^4}))}$$

and the right hand side of this last inequality is < 2 for all $p \geq 5$: for example,

p	bound
3	2.99
5	1.7
17	1.13
31	1.07
101	1.02

However, for $n = 6$ we can show that $f_c(6,4)$ goes to infinity with p.

In [ST68], Suprunenko and Tyshkevich constructed a class of commutative dimension 6 nilpotent algebras N with $N^3 = 0$ over an infinite field F and showed that they form an infinite set of nonisomorphic algebras over F.

In this section we present Suprunenko and Tyshkevich's construction in detail. The construction implies that the number of isomorphism types of commutative dimension 6 nilpotent algebras over $\mathbb{F}_p$ is bounded below by a linear function of p.

More precisely, we consider a class of dimension 6 nilpotent algebras $N = N_\alpha$ with $\dim(N/N^2) = 4$ and $N^3 = 0$, parametrized by elements α of $\mathbb{F}_p$ We show that the orbits of these algebras under the action of $G = \mathrm{GL}_4 \times \mathrm{GL}_2$ contains either six or two such algebras. We obtain a precise count of the number of orbits of these algebras, a count that depends on whether p is congruent to 1 or 5 modulo 6. The number of orbits will depend on p.

Let $N_\alpha = \langle u_1, u_2, u_3, u_4\rangle$, let $\{v_1, v_2\}$ be a basis of N^2, and

$$\begin{aligned} u_1^2 &= v_1 - v_2 \\ u_2^2 &= v_1 \\ u_3^2 &= v_1 + v_2 \\ u_4^2 &= v_1 + \alpha v_2 \\ u_i u_j &= 0 \text{ for all } i \neq j. \end{aligned}$$

Then N_α has structure matrices

$$\Phi^{(1)} = I, \quad \Phi^{(2)} = \operatorname{diag}(-1, 0, 1, \alpha) = A_\alpha.$$

Let $N_\beta = \langle w_1, w_2, w_3, w_4\rangle$, with $\{z_1, z_2\}$ a basis of N^2, and

$$\begin{aligned} w_1^2 &= z_1 - z_2 \\ w_2^2 &= z_1 \\ w_3^2 &= z_1 + z_2 \\ w_4^2 &= z_1 + \beta z_2 \\ w_i w_j &= 0 \text{ for all } i \neq j. \end{aligned}$$

Thus $\Theta^{(1)} = I, \Theta^{(2)} = A_\beta$ are the structure matrices for N_β. Now N_α and N_β are in the same orbit under G if and only if there is an invertible 4×4 matrix P and an invertible 2×2 matrix $Q = (q_{ij})$ so that

$$\begin{aligned} \Theta^{(1)} &= q_{11} P \Phi^{(1)} P^T + q_{21} P \Phi^{(2)} P^T; \\ \Theta^{(2)} &= q_{12} P \Phi^{(1)} P^T + q_{22} P \Phi^{(2)} P^T. \end{aligned}$$

That is,

$$\begin{aligned} I &= q_{11} P P^T + q_{21} P A_\alpha P^T; \\ A_\beta &= q_{12} P P^T + q_{22} P A_\alpha P^T. \end{aligned}$$

We first show that PP^T and $PA_\alpha P^T$ must be diagonal. Let

$$(PP^T)_{ij} = t_{ij}, (PA_\alpha P^T)_{ij} = s_{ij}.$$

Then for $i \neq j$, we have from these last equations:

$$\begin{aligned} 0 &= q_{11} t_{ij} + q_{21} s_{ij} \\ 0 &= q_{12} t_{ij} + q_{22} s_{ij}. \end{aligned}$$

Since Q is invertible, the only solution is $s_{ij} = t_{ij} = 0$.

Thus $PP^T = \operatorname{diag}(c_1, c_2, c_3, c_4)$ is diagonal. If we multiply P by $1/c_1$ and multiply Q by c_1^2, we don't change the equations connecting the structure matrices of N_α and N_β, and may assume that

$$PP^T = \operatorname{diag}(1, p_1, p_2, p_3) = D.$$

Then $PP^T D^{-1} = I$, so $P^T = P^{-1} D$, hence $PA_\alpha P^T = PA_\alpha P^{-1} D$. The eigenvalues of $PA_\alpha P^{-1}$ are the same as those of A_α, namely, $-1, 0, 1$ and

α. So $PA_\alpha P^{-1} = \operatorname{diag}(\alpha_0, \alpha_1, \alpha_2, \alpha_3)$, where $\{\alpha_0, \alpha_1, \alpha_2, \alpha_3\} = \{1, 0, -1, \alpha\}$ (in some unspecified order).

Our two equations above are then

$$\begin{aligned} I &= q_{11} \operatorname{diag}(1, p_1, p_2, p_3) + q_{21} \operatorname{diag}(\alpha_0, \alpha_1 p_1, \alpha_2 p_2, \alpha_3 p_3) \\ \operatorname{diag}(-1, 0, 1, \beta) &= q_{12} \operatorname{diag}(1, p_1, p_2, p_3) + q_{22} \operatorname{diag}(\alpha_0, \alpha_1 p_1, \alpha_2 p_2, \alpha_3 p_3). \end{aligned}$$

Since p_1 is nonzero, the four equations involving α_0 and α_1 are equivalent to

$$\begin{aligned} 1 &= q_{11} + q_{21}\alpha_0 \\ -1 &= q_{12} + q_{22}\alpha_0 \\ 1/p_1 &= q_{11} + q_{21}\alpha_1 \\ 0 &= q_{12} + q_{22}\alpha_1, \end{aligned}$$

which in matrix form becomes

$$\begin{pmatrix} q_{11} & q_{21} \\ q_{12} & q_{22} \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{p_1} \\ -1 & 0 \end{pmatrix} \begin{pmatrix} \alpha_1 & -1 \\ -\alpha_0 & 1 \end{pmatrix}.$$

We can use these to solve for the components of Q in terms of the the α_j, the p_i and β:

$$\begin{aligned} q_{11} &= \left(\frac{1}{\alpha_1 - \alpha_0}\right)\left(\alpha_1 - \frac{\alpha_0}{p_1}\right) \\ q_{12} &= \left(\frac{1}{\alpha_1 - \alpha_0}\right)(-\alpha_1) \\ q_{21} &= \left(\frac{1}{\alpha_1 - \alpha_0}\right)(-1 + 1/p_1) \\ q_{22} &= \frac{1}{\alpha_1 - \alpha_0}. \end{aligned}$$

The remaining four equations involve p_1, p_2, p_3 and β:

$$\begin{aligned} 1 &= q_{11}p_2 + q_{21}\alpha_2 p_2 \\ 1 &= q_{12}p_2 + q_{22}\alpha_2 p_2 \\ 1 &= q_{11}p_3 + q_{21}\alpha_3 p_3 \\ \beta &= q_{12}p_3 + q_{22}\alpha_3 p_3. \end{aligned}$$

These are equivalent to

$$\begin{aligned} \frac{1}{p_2} &= q_{11} + q_{21}\alpha_2 = q_{12} + q_{22}\alpha_2 \\ \frac{1}{p_3} &= q_{11} + q_{21}\alpha_3 = \frac{1}{\beta}(q_{12} + q_{22}\alpha_3). \end{aligned}$$

Substituting for the components of Q gives

$$\begin{aligned}
\frac{1}{p_2} &= \left(\frac{1}{\alpha_1-\alpha_0}\right)\left[\left(\alpha_1-\frac{\alpha_0}{p_1}\right)+\left(-1+\frac{1}{p_1}\right)\alpha_2\right]\\
\frac{1}{p_2} &= \frac{\alpha_2-\alpha_1}{\alpha_1-\alpha_0}\\
\frac{1}{p_3} &= \left(\frac{1}{\alpha_1-\alpha_0}\right)\left[\left(\alpha_1-\frac{\alpha_0}{p_1}\right)+\left(-1+\frac{1}{p_1}\right)\alpha_3\right];\\
\frac{\beta}{p_3} &= \frac{\alpha_3-\alpha_1}{\alpha_1-\alpha_0}.
\end{aligned}$$

We set the two expressions for $1/p_2$ to solve for p_1:

$$\left(\alpha_1-\frac{\alpha_0}{p_1}\right)+\left(-1+\frac{1}{p_1}\right)\alpha_2=\alpha_2-\alpha_1,$$

so

$$p_1=\frac{\alpha_2-\alpha_0}{2(\alpha_2-\alpha_1)}.$$

We also have that

$$p_2=\frac{\alpha_1-\alpha_0}{\alpha_2-\alpha_1}.$$

Substituting for p_1 in the expression for $1/p_3$, we have that

$$\frac{1}{p_3}=\frac{(\alpha_1-\alpha_3)}{(\alpha_2-\alpha_0)+2(\alpha_3-\alpha_0)(\alpha_2-\alpha_1)}(\alpha_2-\alpha_0)(\alpha_1-\alpha_0).$$

So

$$p_3=\frac{(\alpha_1-\alpha_0)(\alpha_2-\alpha_0)}{(\alpha_1-\alpha_3)(\alpha_2-\alpha_0)+2(\alpha_3-\alpha_0)(\alpha_2-\alpha_1)}.$$

Then

$$\begin{aligned}
\beta &= p_3\frac{(\alpha_3-\alpha_1)}{(\alpha_1-\alpha_0)}\\
&= \frac{(\alpha_3-\alpha_1)(\alpha_2-\alpha_0)}{(\alpha_1-\alpha_3)(\alpha_2-\alpha_0)+2(\alpha_3-\alpha_0)(\alpha_2-\alpha_1)}.
\end{aligned}$$

Thus β is uniquely determined, provided that $\alpha\neq -1, 0$ or 1 (which implies that the components of Q, p_1 and p_2 are defined) and the denominator

$$\Delta=(\alpha_1-\alpha_3)(\alpha_2-\alpha_0)+2(\alpha_3-\alpha_0)(\alpha_2-\alpha_1)$$

of p_3 and β is nonzero.

We have 24 cases, corresponding to the 4! possible ways of choosing $\alpha_1,\alpha_2,\alpha_3,\alpha_4$ from $\{-1,0,1,\alpha\}$. The possible ways of choosing $\alpha_0,\alpha_1,\alpha_2$ and α_3, and the corresponding β, are shown in Table 1

As the table shows, each possible permutation of $-1,0,1$ and α yields a unique value of β, provided that the denominators $\Delta=3\alpha\pm 1$ are not zero.

TABLE 1. Values of β.

α_0	α_1	α_2	α_3	Δ	β
-1	0	1	α	2	α
1	0	-1	α	$-3\alpha-1$	$-\alpha$
0	1	-1	α	$3\alpha-1$	$(\alpha-1)/(3\alpha+1)$
0	-1	1	α	$-3\alpha-1$	$(\alpha+1)/(3\alpha-1)$
-1	1	0	α	$3\alpha-1$	$-(\alpha-1)/(3\alpha+1)$
1	-1	0	α	$3\alpha-1$	$-(\alpha+1)/(3\alpha-1)$
-1	0	α	1	$3\alpha-1$	$(\alpha+1)/(3\alpha-1)$
1	0	α	-1	$-3\alpha-1$	$(\alpha-1)/(3\alpha+1)$
0	1	α	-1	2	$-\alpha$
0	-1	α	1	2	α
-1	1	α	0	$3\alpha-1$	$-(\alpha+1)/(3\alpha-1)$
1	-1	α	0	$-3\alpha-1$	$-(\alpha-1)/(3\alpha+1)$
-1	α	0	1	$-3\alpha-1$	$(\alpha-1)/(3\alpha+1)$
1	α	0	-1	$3\alpha-1$	$(\alpha+1)/(3\alpha-1)$
0	α	1	-1	$3\alpha-1$	$-(\alpha+1)/(3\alpha-1)$
0	α	-1	1	$-3\alpha-1$	$-(\alpha-1)/(3\alpha+1)$
-1	α	1	0	2	$-\alpha$
1	α	-1	0	2	α
α	-1	0	1	2	$-\alpha$
α	1	0	-1	2	α
α	0	1	-1	$-3\alpha-1$	$-(\alpha-1)/(3\alpha+1)$
α	0	-1	1	$3\alpha-1$	$-(\alpha+1)/(3\alpha-1)$
α	-1	1	0	$-3\alpha-1$	$(\alpha-1)/(3\alpha+1)$
α	1	-1	0	$3\alpha-1$	$(\alpha+1)/(3\alpha-1)$

The β's are obtained from α by applying the six Mobius transformations that send x to:

$$x, \quad -x, \quad \frac{x-1}{3x+1}, \quad -\frac{x-1}{3x+1}, \quad \frac{x+1}{3x-1}, \quad -\frac{x+1}{3x-1}.$$

It is routine to check that this set M of transformations is closed under composition and is isomorphic to the dihedral group D_3 of order 6. In fact, under the map from $\mathrm{GL}_2(\mathbb{F}_p)$ to M,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \frac{ax+b}{cx+d},$$

the group M is isomorphic to the subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$ represented by the matrices

$$\begin{pmatrix}1&0\\0&1\end{pmatrix}, \quad \begin{pmatrix}-1&0\\0&1\end{pmatrix}, \quad \begin{pmatrix}1&-1\\3&1\end{pmatrix},$$
$$\begin{pmatrix}-1&1\\3&1\end{pmatrix}, \quad \begin{pmatrix}1&1\\3&-1\end{pmatrix}, \quad \begin{pmatrix}-1&-1\\3&-1\end{pmatrix}.$$

Thus we have:

Proposition 9.1. *Let $p \geq 7$ and let $\mathcal{N}$ be the set of six-dimensional nilpotent algebras N_α where α is in $\mathcal{A} = \mathbb{F}_p \setminus \{0, 1, -1, \frac{1}{3}, -\frac{1}{3}\}$. Then the orbit of N_α in $\mathcal{N}$ under the action of $G = \mathrm{GL}_4(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ contains at most six algebras N_β, and each β is in $\mathcal{A}$. Thus there are at least $\lfloor \frac{p-5}{6} \rfloor$ isomorphism types of nilpotent algebras in $\mathcal{N}$.*

Example 9.2. For $p = 7$, the set $\mathcal{A} = \{3, 4\}$ is a single orbit under the action of G.

For $p = 13$, $\mathcal{A}$ partitions into two orbits: $\{2, 11\}$ and $\{3, 10, 5, 8, 6, 7\}$.

For $p = 19$, $\mathcal{A}$ partitions into three orbits:

$$\{2, 17, 7, 12, 8, 11\}, \quad \{3, 16, 4, 15, 9, 10\} \quad \text{and} \quad \{5, 14\}.$$

For $p = 41$, $\mathcal{A}$ partitions into six orbits:

$$\{2, 39, 6, 35, 17, 24\}, \quad \{4, 37, 7, 34, 16, 25\},$$
$$\{3, 38, 8, 33, 20, 21\}, \quad \{5, 36, 10, 31, 18, 23\}$$
$$\{9, 32, 12, 29, 13, 28\}, \quad \{11, 30, 15, 26, 19, 22\}.$$

(Omitted from $\mathcal{A}$ for $p = 41$ are 0, 1, $14 = 1/3$, $27 = -1/3$ and $-1 = 40$.)

These examples generalize to give a more precise result.

Theorem 9.3. *Let $\mathcal{A} = \mathbb{F}_p \setminus \{-1, 0, 1, 1/3, -1/3\}$. If $p = 6k + 5$, then there are exactly k orbits in $\mathcal{A}$ under the action of G, and hence there are $k = \frac{p-5}{6}$ isomorphism types of nilpotent algebras N_α over $\mathbb{F}_p$. If $p = 6k + 1$, then there are $k - 1$ orbits of size 6 and one orbit of size 2 in $\mathcal{A}$. Thus there are $k = \frac{p-1}{6}$ isomorphism types of nilpotent algebras N_α over $\mathbb{F}_p$.*

Proof. One checks that α is in an orbit of size 2 if and only if

$$\alpha = \frac{\alpha - 1}{3\alpha - 1} = -\frac{\alpha + 1}{3\alpha - 1}$$

iff

$$-\alpha = -\frac{\alpha - 1}{3\alpha - 1} = \frac{\alpha + 1}{3\alpha - 1}$$

iff

$$3\alpha^2 = -1.$$

Any other equalities among

$$\pm\alpha, \quad \pm\frac{\alpha - 1}{3\alpha - 1}, \quad \pm\frac{\alpha + 1}{3\alpha - 1}$$

yield excluded values of α (namely $\alpha = 0$, 1, -1, $1/3$, $-1/3$).

Now the equation

$$3\alpha^2 = -1$$

has a solution in $\mathbb{F}_p$ iff the Legendre symbol $\left(\frac{-3}{p}\right) = 1$, iff $p \equiv 1 \pmod 6$. In that case, there is one orbit containing the two square roots of $-1/3$ in $\mathbb{F}_p$. If $p \equiv 5 \pmod 6$, then the five nontrivial Mobius transformations have no fixed points, so the orbit of each N_α contains six N_β. □

10. An asymptotic estimate for $t_n(G)$ for large n

We seek an estimate for $t_n(G)$, the number of Hopf Galois structures of type G on a Galois extension L/K with Galois group $G \cong \mathbb{F}_p^n$, for large n.

For a lower bound on that number, we start with a lower bound on the number of isomorphism classes of commutative $\mathbb{F}_p$-algebras N of dimension n with $N^3 = 0$, where r can vary. All such algebras correspond to regular subgroups of $\mathrm{Hol}(G)$ isomorphic to G, as noted earlier.

To do so, we find the maximum of the lower bound exponent

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

over r with $0 < r < n$.

Write $r = tn$ for $0 < t < 1$ and let

$$c(t) = -2b(t)/n^2 = nt^3 - 2nt^2 + 5t^2 - 5t + 2.$$

To find the maximum value of $c(t)$ for $0 < t < 1$, differentiate $c(t)$ to get

$$c'(t) = 3nt^2 - 2nt + 10t - 5,$$

which is zero for

$$t = \frac{1}{3} - \frac{5}{3n} + \frac{1}{3}\sqrt{1 + \frac{5}{n} + \frac{25}{n^2}}.$$

For various n, the t for which $c(t)$ is maximum is

n	t
3	.556
6	.586
10	.608
20	.632
50	.651
100	.659
500	.665
1000	.666
5000	.667

For large n the value of t where $b(t)$ is maximum converges to $2/3$. As noted earlier, for $r = 2n/3$,

$$b = \frac{2}{27}n^3 - \frac{4}{9}n^2.$$

So

Proposition 10.1. *The number of commutative $\mathbb{F}_p$-algebras N of dimension n with $N^3 = 0$ is at least*

$$p^{\max\{b(t)\}}$$

and for $n \to \infty$, $\max\{b(t)\}$ converges to $\frac{2}{27}n^3 - \frac{4}{9}n^2$.

For an upper bound, we cite Poonen ([Po08a], Theorem 10.9):

Theorem 10.2. *The number of isomorphism classes of pairs (N, ϕ) where N is nilpotent commutative $\mathbb{F}_p$-algebra of rank n and $\phi : N \to \mathbb{F}_p^n$ is an isomorphism that defines a fixed ordered basis of N, is $p^{\frac{2}{27}n^3+O(n^{8/3})}$ as $n \to \infty$.*

Forgetting the basis structure reduces the number of isomorphism classes. So the number of isomorphism types of nilpotent commutative algebras of rank n is bounded from above by $p^{\frac{2}{27}n^3+O(n^{8/3})}$ as n goes to infinity. We have the following inequalities:

$$\begin{aligned}
&|\{\text{isomorphism types of commutative } \mathbb{F}_p\text{-algebras } N \text{ with } N^3 = 0\}| \\
&\leq |\{\text{isomorphism types of commutative } \mathbb{F}_p\text{-algebras } N \text{ with } N^p = 0\}| \\
&\leq |\{\text{isomorphism types of commutative nilpotent } \mathbb{F}_p\text{-algebras } N\}| \\
&\leq |\{\text{isomorphism types of pairs } (N, \phi) \text{ as above.}|
\end{aligned}$$

The second term,

$$|\{\text{isomorphism types of commutative } \mathbb{F}_p\text{-algebras } N \text{ with } N^p = 0\}|,$$

is equal to the number $\mathcal{O}_G$ of orbits in $\mathrm{Hol}(\mathbb{F}_p^n)$ under conjugation where the orbits contain regular subgroups isomorphic to $G = \mathbb{F}_p^n$. Thus as $n \to \infty$,

$$p^{\frac{2}{27}n^3-\frac{4}{9}n^2} \leq \mathcal{O}_G \leq p^{\frac{2}{27}n^3+O(n^{8/3})}.$$

As n goes to infinity, the number of orbits of regular subgroups of $\mathrm{Hol}(G)$ isomorphic to G is asymptotic to $p^{\frac{2}{27}n^3}$.

We can then approach the question: For n large, if L/K is a Galois extension with Galois group $G \cong (\mathbb{F}_p^n, +)$ an elementary abelian p-group, how many abelian Hopf Galois structures are there on L/K of type G?

To obtain an estimate of the number of abelian Hopf Galois structures on L/K of type G, observe that for each regular subgroup J isomorphic to $C_p^n \cong \mathbb{F}_p^n$, the number of equivalence classes of isomorphisms $\beta : G \to J$ is

$$\frac{|\mathrm{GL}_n(\mathbb{F}_p)|}{|\mathrm{Sta}(J)|},$$

and the size of that number is bounded above by $|\mathrm{M}_n(\mathbb{F}_p)| = p^{n^2}$ and below by 1.

Applying those bounds, Theorem 1.2 and the lower and upper bounds on nilpotent commutative algebras N with $N^p = 0$ just noted, we see that

the number $t_n(G)$ of Hopf Galois structures of type G on a Galois extension L/K with Galois group $G = C_p^n$, p odd, satisfies

$$p^{\frac{2}{27}n^3-\frac{4}{9}n^2} < t_n(G) < p^{\frac{2}{27}n^3+O(n^{8/3})} \cdot p^{n^2}.$$

Hence:

Theorem 10.3. *The number $t_n(G)$ of Hopf Galois structures of type G on a Galois extension L/K with Galois group $G = C_p^n$, p odd, is asymptotic to*

$$p^{\frac{2}{27}n^3}$$

as $n \to \infty$.

The size of the stabilizer is asymptotically irrelevant.

Of course for small n the orders of stabilizers is required for precise counts.

For $n = 3$ we found in [Ch05] the orders of the stabilizers of each of the five representative regular subgroups. (The fact that those stabilizers had different orders insured that the orbits of the five representative subgroups were all different.) Finding the orders of the stabilizers yielded in [Ch05, Theorem 7.2] the number $t_3(G)$ of Hopf Galois structures of type G on a Galois extension L/K with Galois group $G = C_p^3$, namely $s = p^6 + p^5 - p^2$.

But except for the special class, studied in the final section of [Ch07], of regular subgroups corresponding to the nilpotent algebras N of dimension n with $\dim(N^i/N^{i+1}) = 1$ for all i, almost nothing precise is known about stabilizers of regular subgroups of $\mathrm{Hol}(G)$ where $G = \mathbb{F}_p^n$ and $n \geq 4$. We leave that problem for further research.

References

[BW66] Beightler, Charles S.; Wilde, Douglass J. Diagonalization of quadratic forms by Gauss elimination. *Management Sci.* **12** (1966), 371–379. MR0189225 (32 #6652), Zbl 0144.42804, doi: 10.1287/mnsc.12.5.371.

[BM53] Birkhoff, Garrett; Mac Lane, Saunders. A survey of modern algebra. Rev. ed. *Macmillan Co., New York, N. Y.*, 1953. xi+472 pp. MR0054551 (14,939a), Zbl 0052.25402.

[By96] Byott, N. P. Uniqueness of Hopf Galois structure for separable field extensions. *Comm. Algebra* **24** (1996), no. 10, 3217–3228. MR1402555 (97j:16051a), Zbl 0878.12001, doi: 10.1080/00927879608825743.

[CDVS06] Caranti, A.; Dalla Volta, F.; Sala, M. Abelian regular subgroups of the affine group and radical rings. *Publ. Math. Debrecen* **69** (2006), no. 3, 297–308. MR2273982 (2007j:20001), Zbl 1123.20002, arXiv:math/0510166, doi: 10.1017/S0004972708001068.

[Ch05] Childs, Lindsay N. Elementary abelian Hopf Galois structures and polynomial formal groups. *J. Algebra* **283** (2005), no. 1, 292–316. MR2102084 (2005g:16073), Zbl 1071.16031, doi: 10.1016/j.jalgebra.2004.07.009.

[Ch07] Childs, Lindsay N. Some Hopf Galois structures arising from elementary abelian p-groups. *Proc. Amer. Math. Soc.* **135** (2007), no. 11, 3453–3460. MR2336557 (2008j:16107), Zbl 1128.16022, doi: 10.1090/S0002-9939-07-08888-0.

[deG10] de Graaf, Willem A. Classification of nilpotent associative algebras of small dimension. Preprint, 2010. arXiv:1009.5339.

[Fe03] Featherstonhaugh, S. C. Abelian Hopf Galois extensions of Galois field extensions of prime power order. Ph. D. thesis, Univ. at Albany, NY, 2003.

[FCC12] Featherstonhaugh, S. C.; Caranti, A.; Childs, L. 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.

[GP87] Greither, Cornelius; Pareigis, Bodo. Hopf Galois theory for separable field extensions. *J. Algebra* **106** (1987), no. 1, 239–258. MR0878476 (88i:12006), Zbl 0615.12026, doi: 10.1016/0021-8693(87)90029-9.

[Ka69] Kaplansky, Irving. Linear algebra and geometry. A second course. *Allyn and Bacon, Inc., Boston, Mass.* 1969. xii+139 pp. MR0249444 (40 #2689), Zbl 0184.24201.

[KP69] Kruse, Robert L.; Price, David T. Nilpotent rings. *Gordon and Breach Science Publishers, New York-London-Paris* 1969. viii+127 pp. paperbound. MR0266956 (42 #1858), Zbl 0198.36102.

[KP70] Kruse, Robert L.; Price, David T. Enumerating finite rings. *J. London Math. Soc.* (2), **2** (1970), 149–159. MR0251079 (40 #4310), Zbl 0188.08601, doi: 10.1112/jlms/s2-2.1.149.

[Maz80] Mazzola, Guerino. Generic finite schemes and Hochschild cocycles. *Comment. Math. Helv.* **55** (1980), no. 2, 267–293. MR0576606 (82k:14010), Zbl 0463.14004, doi: 10.1007/BF02566686.

[Po08a] Poonen, Bjorn. The moduli space of commutative algebras of finite rank. *J. Eur. Math. Soc.* **10** (2008), no. 3, 817–836. MR2421162 (2009d:14009), Zbl 1151.14011, arXiv:math/0608491, doi: 10.4171/JEMS/131.

[Po08b] Poonen, Bjorn. Isomorphism types of commutative algebras of finite rank over an algebraically closed field. *Computational arithmetic geometry*, 111–120, Contemp. Math., 463. *Amer. Math. Soc., Providence, RI*, 2008. MR2459993 (2010c:13018), Zbl 1155.13015, doi: 10.1090/conm/463/09050.

[ST68] Suprunenko, D. A.; Tyškevič, R. I. Commutative matrices. *Academic Press, New York, NY*, 1968.

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

This paper is available via http://nyjm.albany.edu/j/2015/21-10.html.