New York Journal of Mathematics

New York J. Math. **20** (2014) 779–797.

Hopf Galois structures on primitive purely inseparable extensions

Alan Koch

Abstract. Let L/K be a primitive purely inseparable extension of fields of characteristic p, $[L:K] > p$, p odd. It is well known that L/K is Hopf Galois for some Hopf algebra H, and it is suspected that L/K is Hopf Galois for numerous choices of H. We construct a family of K-Hopf algebras H for which L is an H-Galois object. For some choices of K we will exhibit an infinite number of such H. We provide some explicit examples of the dual, Hopf Galois, structure on L/K.

Contents

Let K be a field of characteristic $p \geq 3$. Let L be a field which is a tensor product of simple field extensions over K. Then L/K is called modular. In [1], Chase shows that L is a principal homogeneous space for some infinitesimal K-group scheme G. If $G = \operatorname{Spec} H$ then H is a finite dimensional, commutative, cocommutative K-Hopf algebra which is local with local linear dual (hereafter, "local-local"), and L is an H-Galois object. Interpreted using duality, this shows that L/K is a Hopf Galois extension for H^*, the dual Hopf algebra to H, which is also a finite dimensional, commutative, cocommutative, local-local K-Hopf algebra.

A natural question arises: for a given extension L/K, is it Hopf Galois for a unique choice of H? It is well-known that the answer to this question is "no". Modular extensions are, by their definition, purely inseparable. In the work cited above, Chase writes "[s]crutiny of the simplest examples shows

Received July 22, 2014.

2010 *Mathematics Subject Classification.* 16T05.

Key words and phrases. Hopf algebras, Hopf Galois extensions, purely inseparable extensions.

ISSN 1076-9803/2014

that a modular extension can be a PHS for many different truncated $[K]$-group schemes G." This comment suggests that L is an H-Galois object for many choices of H.

The question is then modified: for a given extension L/K, can we describe all of the Hopf algebras which make it Hopf Galois? The separable analogue, where L/K is a separable extension, is definitively answered in [4], which describes all such H using group theory. The Hopf algebras in the separable case correspond to a certain class of regular subgroups of the group of permutations $\mathrm{Perm}(\mathrm{Gal}\,(E/K)\,/\,\mathrm{Gal}\,(L/K)) \cong S_n$, where $n = [L:K]$ and E is a Galois closure of L/K, which are normalized by the subgroup of $\mathrm{Perm}(\mathrm{Gal}\,(E/K)\,/\,\mathrm{Gal}\,(L/K))$ obtained by the left translations by $\mathrm{Gal}\,(E/K)$. This elegant result shows that the classification of Hopf Galois structures depends not on the fields but on the group. Clearly the number of such Hopf algebras is finite.

In this work, we focus primarily on the simplest class of modular extensions, namely the primitive extensions. We will construct a family of monogenic K-Hopf algebras ("monogenic" means generated as a K-algebra by a single element) of dimension equal to $[L:K] = p^n$, $n \geq 2$, and show that each makes L into a Hopf Galois object. These Hopf algebras fall into $n-1$ classes, and the r^{th} class is parameterized by elements of $K^\times/(K^{p^{r+1}-1})^\times$. Not only is L an H-Galois object for each of our constructed Hopf algebras, the realization of L as an H-Galois object can be done in multiple ways: we will explicitly describe $p^{n-1}\,(p-1)$ such coactions. Unlike the separable case, the number of Hopf Galois extensions evidently depends on the fields; in particular, our work will produce examples where the extension L/K is Hopf Galois for an infinite number of Hopf algebras.

We will also briefly discuss general modular extensions. The work presented in the simple case extends to modular extensions quite easily, however we will show that there are modular extensions which are H-Galois objects for Hopf algebras which cannot be constructed in the manner presented here.

It should be noted that these constructions can also be done geometrically, using the language of group schemes and principal homogeneous spaces (or "torsors"). Indeed, the Hopf algebras we construct represent certain subgroups of group schemes of finite length Witt vectors. We have opted to present our results using a purely algebraic approach for three reasons. First, the language in [4] is one of Hopf algebras and Hopf-Galois extensions, and as we are investigating an inseparable analogue to the results in that paper it seems natural to try to use the same language as much as possible. Second, we feel the question is stated more naturally using Hopf algebras — "given a field extension L/K, for which Hopf algebras is it a Hopf Galois extension" makes the point more directly than "for $\mathrm{Spec}\,K \to \mathrm{Spec}\,L$, L a field, for which group schemes G does $\mathrm{Spec}\,L$ appear as a torsor?" does. Third, in [8] we use these Hopf algebras to describe the ring of integers in

the case where L and K are local fields; an explicit description of the Hopf algebra action is necessary in that work.

Throughout, p is a fixed odd prime and K is an imperfect field containing a perfect field k of characteristic p. (For example, K could be the function field $\mathbb{F}_p(t)$ or the field of Laurent series $\mathbb{F}_p((t))$.) All unadorned tensors are over K. We denote by $K^{p^{-\infty}}$ the perfect closure of K in some algebraic closure. All rings (and algebras) are assumed to be commutative. All Hopf algebras are assumed to be finite, commutative, cocommutative, of p-power rank, and local-local.

Acknowledgements. The author would like to thank Nigel Byott and Lindsay Childs for their input during the creation of this paper, as well as the referee for his detailed comments on the original version of this manuscript.

1. Background

We briefly describe the notion of Hopf Galois extensions and Hopf Galois objects. More details can be found, e.g., in [2]. Let H be a K-Hopf algebra, comultiplication Δ and counit ε. We say that L is an H-module algebra if L is an H-module such that for all $a, b \in L$ and $f \in K$ we have

$$h(ab) = \operatorname{mult} \Delta(h)(a \otimes b)$$
$$h(f) = \varepsilon(h) f.$$

If furthermore the K-linear map $L \otimes H \to \operatorname{End}_K(L)$, $(a \otimes h) \mapsto (b \mapsto ah(b))$ is an isomorphism, then we say L/K is an H-Galois extension, or simply Hopf Galois if the Hopf algebra is understood. This can be seen as a generalization of the usual Galois theory: if E/F is a Galois extension, $\Gamma = \operatorname{Gal}(E/F)$ then E/F is Hopf Galois via the group algebra $F[\Gamma]$.

Loosely, the notion of a Hopf Galois object is dual to that of a Hopf Galois extension. Given a K-Hopf algebra H, suppose there is a K-algebra map $\alpha : L \to L \otimes H$ such that

$$(\alpha \otimes 1)\alpha = (1 \otimes \Delta)\alpha : L \to L \otimes H \otimes H$$
$$\operatorname{mult}(1 \otimes \varepsilon)\alpha = \mathrm{id}_L.$$

Then L is said to be an H-comodule algebra. If furthermore the map $\gamma : L \otimes L \to L \otimes H$ given by $\gamma(a \otimes b) = (a \otimes 1)\alpha(b)$ is an isomorphism, then L is an H-Galois object (or H-principal homogeneous space). It can be shown that L/K is H-Galois if and only if L is an H^*-Galois object, where $H^* = \operatorname{Hom}_K(H, K)$ is the linear dual to H.

In the sections that follow, we construct Hopf algebras H for which L is an H-Galois object. Dualizing will put H^*-Galois structures on L/K.

The construction of both the comultiplication maps Δ and coaction maps α that follow rely heavily on Witt vector addition. Much of the background on Witt vectors can be found in [5]. For the convenience of the reader we

will briefly recall the construction and illustrate some its properties which will be necessary for the rest of the paper.

For each positive integer d, define

$$w_d(Z_0,\dots,Z_d) = Z_0^{p^d} + pZ_1^{p^{d-1}} + \cdots + p^d Z_d \in \mathbb{Z}[Z_0,\dots,Z_d].$$

The polynomials w_d are called Witt polynomials. Define

$$S_d := S_d((X_0,\dots,X_d);(Y_0,\dots,Y_d))$$

recursively by

$$w_d(S_0,\dots,S_d) = w_d(X_0,\dots,X_d) + w_d(Y_0,\dots,Y_d),$$

i.e.,

$$S_d = \frac{1}{p^d}\left(w_d(X_0,\dots,X_d) + w_d(Y_0,\dots,Y_d) - S_0^{p^d} - S_1^{p^{d-1}} - \cdots - S_{d-1}^{p}\right).$$

Clearly $S_d \in \mathbb{Q}[X_0,\dots,X_d,Y_0,\dots,Y_d]$; a less obvious, but fundamental, result is that we in fact have $S_d \in \mathbb{Z}[X_0,\dots,X_d,Y_0,\dots,Y_d]$. To give two explicit examples of these polynomials,

$$S_0(X_0;Y_0) = X_0 + Y_0$$

$$S_1((X_0,X_1);(Y_0,Y_1)) = X_1 + Y_1 - \sum_{i=1}^{p-1} \frac{(p-1)!}{i!\,(p-i)!} X_0^i Y_0^{p-i}.$$

Let $W(\mathbb{Z}) = \{(a_0,a_1,\dots) : a_i \in \mathbb{Z}\}$, and define a binary operation on $W(\mathbb{Z})$ by

$$(a_0,a_1,\dots) + (b_0,b_1,\dots) = (S_0(a_0;b_0), S_1((a_0,a_1);(b_0,b_1)),\dots).$$

Then $W(\mathbb{Z})$ is a group: the identity is $(0,0,\dots)$ and the additive inverse is obtained by negating the components. This is typically proved by observing that the map

$$W(\mathbb{Z}) \to \prod_{i=0}^{\infty} \mathbb{Z}$$
$$(a_0,a_1,\dots) \to (w_0(a_0), w_1(a_0,a_1),\dots)$$

is a bijection from which $W(\mathbb{Z})$ inherits its structure from the product on the right. As $W(\mathbb{Z})$ is a group, the component operation S_d is associative for all d.

By replacing $\mathbb{Z}$ with a $\mathbb{Z}$-algebra R, we obtain the group $W(R)$. The polynomials S_d can then be viewed as elements of $R[X_0,\dots,X_d,Y_0,\dots,Y_d]$. In fact, for any commutative ring R we may view W as an R-group scheme.

We conclude this section by recording two well-known observations which will be needed later. The first equality holds because S_d is a polynomial expression in $x_0,\dots,x_d,y_0,\dots,y_d$. The second follows from that fact that $S_d((X_0,\dots X_d);(Y_0,\dots Y_d))$ is a homogeneous polynomial of degree p^d, where X_i and Y_i each have weight p^i, $0 \le i \le d$.

Lemma 1.1. *Let A and B be K-algebras. Let $f : A \to B$ be a K-algebra map. Then, for $(x_0, x_1 \dots), (y_0, y_1, \dots) \in W(A)$, $c \in K$ we have, for all d,*

$$\begin{aligned} &f(S_d((x_0,\dots,x_d);(y_0,\dots,y_d))) \\ &\qquad = S_d\left((f(x_0),\dots,f(x_d));(f(y_0),\dots,f(y_d))\right) \in B \\ &cS_d((x_0,\dots,x_d);(y_0,\dots,y_d)) \\ &\qquad = S_d\left(\left(c^{p^{-d}}x_0,\dots,cx_d\right);\left(c^{p^{-d}}y_0,\dots,cy_d\right)\right) \in A \end{aligned}$$

Remark 1.2. Since K is not perfect, it is possible that $c^{p^{-i}} \notin K$. However, we may view these as elements of $K^{p^{-\infty}}$.

2. Monogenic Hopf algebras

The objective of this section is to introduce a new family of monogenic K-Hopf algebras. We will accomplish this by generalizing a classification of monogenic k-Hopf algebras (recall k is perfect). We do not claim that our adaptation to K yields all monogenic Hopf algebras.

First, we briefly describe the collection of monogenic Hopf algebras over k. This classification appears in Dieudonné module form in [6] and explicit Hopf algebra descriptions are given in [7].

Fix a positive integer n. By [9, 14.4], all monogenic Hopf algebras of rank p^n share the same k-algebra structure, namely $H = k[t]/\left(t^{p^n}\right)$, so a study of Hopf algebra structures reduces to studying the various comultiplications one can put on this k-algebra. The simplest comultiplication can be obtained by letting $\Delta(t) = t \otimes_k 1 + 1 \otimes_k t$ — that is, t is a primitive element. The others are best described using Witt vector addition polynomials.

Let $0 < r < n$. For $\eta \in k^\times$, define a sequence $\{\eta_i : i \in \mathbb{Z}^+\}$ recursively by

$$\begin{aligned} \eta_1 &= \eta \\ \eta_i &= \eta^{p^{1-i}}\eta_{i-1}^{p^r}. \end{aligned}$$

Notice that the η_i implicitly depend on r. Explicitly, we have $\eta_i = \eta^{e_i}$, where

$$e_i = p^{-(i-1)} + p^{r-(i-2)} + p^{2r-(i-3)} + \cdots + p^{(i-1)r} = \sum_{j=0}^{i-1} p^{jr-(i-j-1)}. \tag{1}$$

Let $H = k[t]/\left(t^{p^n}\right)$, and let $d = \lceil n/r \rceil - 1$. Define $\Delta : H \to H \otimes_k H$ by

$$\begin{aligned} \Delta(t) = S_d\Big(&\left(\eta_d t^{p^{dr}} \otimes_k 1,\dots,\eta_1 t^{p^r} \otimes_k 1, t \otimes_k 1\right); \\ &\left(1 \otimes_k \eta_d t^{p^{dr}},\dots,1 \otimes_k \eta_1 t^{p^r}, 1 \otimes_k t\right)\Big). \end{aligned}$$

This gives H the structure of a k-Hopf algebra with counit $\varepsilon(t) = 0$ and antipode $\lambda(t) = -t$. We will denote this Hopf algebra by $H_{n,r,\eta}$. To see

that the Hopf algebra axioms are satisfied, first notice that coassociativity follows from the associativity of S_d. Also we use Lemma 1.1 to obtain

$$
\begin{aligned}
(2) \qquad \operatorname{mult}(1\otimes\varepsilon)\Delta(t) &= S_d\left(\left(\eta_d t^{p^{dr}},\ldots,t\right);\left(\eta_d\varepsilon(t)^{p^{dr}},\ldots,\varepsilon(t)\right)\right)\\
&= S_d\left(\left(\eta_d t^{p^{dr}},\ldots,t\right);(0,\ldots 0)\right)\\
&= 0,\\
\operatorname{mult}(1\otimes\lambda)\Delta(t) &= S_d\left(\left(\eta_d t^{p^{dr}},\ldots,t\right);\left(\eta_d\lambda(t)^{p^{dr}},\ldots,\lambda(t)\right)\right)\\
&= S_d\left(\left(\eta_d t^{p^{dr}},\ldots,t\right);\left(-\eta_d t^{p^{dr}},\ldots,-t\right)\right)\\
&= 0\\
&= \iota\varepsilon(t),
\end{aligned}
$$

where $\iota : K \to H$ is the K-algebra structure map.

It is shown in [6] that all of the monogenic local-local Hopf algebras of dimension p^n are of the form $H_{n,r,\eta}$. Furthermore, $H_{n,r',\eta'} \cong H_{n,r,\eta}$ if and only if $r = r'$ and $\eta'/\eta = \beta^{p^r - p^{-1}}$ for some $\beta \in k$. In the case where k is finite, this allows us to count the number of monogenic Hopf algebras [6, Cor. 3.2]. On the other hand, if k is algebraically closed, there are exactly n monogenic Hopf algebras of rank p^n.

Now, we adapt the classification in the perfect field case to the case where K contains k and is imperfect. Certainly, $H_{n,r,\eta}\otimes_k K$ is a K-Hopf algebra of dimension p^n. However, a careful reading of the results above reveals that η can be replaced by a more general element of K.

Pick $0 < r < n$. Let $g \in \left(K^{p^{-\infty}}\right)^{\times}$ and define

$$g_1 = g,\ g_i = g^{p^{1-i}} g_{i-1}^{p^r},\ i > 1.$$

Note that $g_i \notin K$ in general, even if $g \in K$. However, it can easily be shown that if $g^p \in K$ then $g_i^{p^i} \in K$.

Our strategy will be to construct a comultiplication Δ on $H = K[t]/\left(t^{p^n}\right)$ such that

$$
\begin{aligned}
&\Delta(t)\\
&= S_d\left(\left(g_d t^{p^{dr}}\otimes 1,\ldots,g_1 t^{p^r}\otimes 1, t\otimes 1\right);\left(1\otimes g_d t^{p^{dr}},\ldots,1\otimes g_1 t^{p^r},1\otimes t\right)\right)
\end{aligned}
$$

for $g \in K^{1/p}$ (although the final form will differ slightly from this). In order to do so, we need to prove that the expression above is an element of $H\otimes H$. The following result accomplishes this.

Lemma 2.1. *Let $g \in K^{1/p}$, and let $\{g_i\}$ be defined as above. Then for all $d \geq 0$,*

$$S_d\left(\left(g_d u^{p^{dr}},\ldots,g_1 u^{p^r},u\right);\left(g_d v^{p^{dr}},\ldots,g_1 v^{p^r},v\right)\right) \in K[u,v].$$

Proof. In a manner similar to Equation (1) we have

$$g_i = g^{e_i}, e_i = p^{-i+1}\sum_{j=1}^{i} p^{(j-1)(r+1)}$$

for all $1 \leq i \leq d$. Thus,

$$g_i = g^{p^{-i+1}g^{\sum_{j=1}^{i} p^{(j-1)(r+1)}}},$$

and the second factor, which we will denote by g_i', is in K. Then

$$g_i = (g^p)^{p^{-i}} g_i',$$

and by Lemma 1.1 we can factor g^p out of

$$S_d\left(\left(g_d u^{p^{dr}}, \ldots, g_1 u^{p^r}, u\right); \left(g_d v^{p^{dr}}, \ldots, g_1 v^{p^r}, v\right)\right)$$

and obtain

$$\begin{aligned} &S_d\left(\left(g_d u^{p^{dr}}, \ldots, g_1 u^{p^r}, u\right); \left(g_d v^{p^{dr}}, \ldots, g_1 v^{p^r}, v\right)\right) \\ &= S_d\left(\left(g_d u^{p^{dr}}, \ldots, g_1 u^{p^r}, g^p g^{-p} u\right); \left(g_d v^{p^{dr}}, \ldots, g_1 v^{p^r}, g^p g^{-p} v\right)\right) \\ &= g^p S_d\left(\left(g_d' u^{p^{dr}}, \ldots, g_1' u^{p^r}, g^{-p} u\right); \left(g_d' v^{p^{dr}}, \ldots, g_1' v^{p^r}, g^{-p} v\right)\right) \end{aligned}$$

Since $g^p, g^{-p}, g_i' \in K$ for all i,

$$S_d\left(\left(g_d u^{p^{dr}}, \ldots, g_1 u^{p^r}, u\right); \left(g_d v^{p^{dr}}, \ldots, g_1 v^{p^r}, v\right)\right) \in K[u, v]. \qquad \square$$

By picking $g \in K^{1/p}$ we get a well-defined algebra map on H using the lemma above with $u = t \otimes 1,\ v = 1 \otimes t$. However, we obtain a nicer parameterization of these maps by letting $f = g^p \in K^\times$. Let

$$f_1 = f^{1/p}, \quad f_i = f_1^{p^{1-i}} f_{i-1}^{p^r} = f^{p^{-i}} f_{i-1}^{p^r}.$$

Proposition 2.2. *Let $0 < r < n$ be integers. Let $d = \lceil n/r \rceil - 1$. Let $f \in K^\times$. Let $f_1, f_2, \ldots, f_d$ be the sequence given recursively by*

$$f_1 = f^{1/p},\ f_i = f^{p^{-i}} f_{i-1}^{p^r},\ i \geq 2$$

as above. Let $H_{n,r,f}$ be the K-algebra $K[t]/\left(t^{p^n}\right)$, and let

$$\begin{aligned} \Delta(t) &= S_d\Big(\left(f_d t^{p^{dr}} \otimes 1, \ldots, f_1 t^{p^r} \otimes 1, t \otimes 1\right); \\ &\qquad \left(1 \otimes f_d t^{p^{dr}}, \ldots, 1 \otimes f_1 t^{p^r}, 1 \otimes t\right)\Big) \\ \varepsilon(t) &= 0 \\ \lambda(t) &= -t \end{aligned}$$

Then these maps endow $H_{n,r,f}$ with the structure of a K-Hopf algebra.

Proof. Since the comultiplication is accomplished using Witt vector sums, the computations here are the same as in Equation (2). Alternatively, we could use the facts that $H_{n,r,f} \otimes K^{p^{-\infty}}$ is a Hopf algebra by [6], and $\Delta(t), \varepsilon(t)$, and $\lambda(t)$ are defined over K. □

3. Isomorphism questions

The Hopf algebras $\{H_{n,r,f} : 0 < r < n,\ f \in K^\times\}$ constructed in Proposition 2.2 are not all unique. While n and r are isomorphism invariants, different choices of f can lead to isomorphic Hopf algebras. Here, we will give a sufficient condition on f, f' for $H_{n,r,f} \cong H_{n,r,f'}$. Additionally, if r is sufficiently large (with respect to n) then we will see this condition is necessary as well.

Suppose $H_{n,r,f} = K[t]/\left(t^{p^n}\right)$. Pick $g \in K^\times$, and let $u = gt$. Then, as a K-algebra, $H_{n,r,f} = K[u]/\left(u^{p^n}\right)$; with the help of Lemma 1.1 we have

$$\begin{aligned}
\Delta(u) &= g\Delta(t) \\
&= gS_d\Big(\Big(f_d t^{p^{dr}} \otimes 1, \ldots, f_1 t^{p^r} \otimes 1, t \otimes 1\Big); \\
&\quad \Big(1 \otimes f_d t^{p^{dr}}, \ldots, 1 \otimes f_1 t^{p^r}, 1 \otimes t\Big)\Big) \\
&= S_d\Big(\Big(g^{p^{-d}} f_d t^{p^{dr}} \otimes 1, \ldots, g^{p^{-1}} f_1 t^{p^r} \otimes 1, gt \otimes 1\Big); \\
&\quad \Big(1 \otimes g^{p^{-d}} f_d t^{p^{dr}}, \ldots, 1 \otimes g^{p^{-1}} f_1 t^{p^r}, 1 \otimes gt\Big)\Big) \\
&= S_d\Big(\Big(g^{p^{-d}-p^{dr}} f_d (gt)^{p^{dr}} \otimes 1, \ldots, g^{p^{-1}-p^r} f_1 (gt)^{p^r} \otimes 1, gt \otimes 1\Big); \\
&\quad \Big(1 \otimes g^{p^{-d}-p^{dr}} f_d (gt)^{p^{dr}}, \ldots, g^{p^{-1}-p^r} f_1 (gt)^{p^r} t^{p^r}, 1 \otimes gt\Big)\Big) \\
&= S_d\Big(\Big(g_d f_d u^{p^{dr}} \otimes 1, \ldots, g_1 f_1 u^{p^r} \otimes 1, u \otimes 1\Big); \\
&\quad \Big(1 \otimes g_d f_d u^{p^{dr}}, \ldots, g_1 f_1 u^{p^r}, 1 \otimes u\Big)\Big),
\end{aligned}$$

where $g_i = g^{p^{-i}-p^{ir}}$. Now

$$\begin{aligned}
g_1^{p^{1-i}} g_{i-1}^{p^r} &= \left(g^{p^{-1}-p^r}\right)^{p^{1-i}} \left(g^{p^{-(i-1)}-p^{(i-1)r}}\right)^{p^r} \\
&= g^{p^{-i}-p^{r+1-i}} g^{p^{r+1-i}-p^{ir-r+r}} \\
&= g^{p^{-i}-p^{ir}} \\
&= g_i,
\end{aligned}$$

and

$$g_1^p = \left(g^{p^{-1}-p^r}\right)^p = g^{1-p^{r+1}}.$$

Thus, replacing f with $fg^{1-p^{r+1}}$ results in the same comultiplication. From this it follows that $H_{n,r,f} \cong H_{n,r,\left(g^{1-p^{r+1}}\right)f}$. More generally,

Proposition 3.1. *Let $f, f' \in K^\times$. Then $H_{n,r,f} \cong H_{n,r,f'}$ if and only if $f/f' \in (K^\times)^{p^{r+1}-1}$.*

Proof. The statement that $H_{n,r,f} \cong H_{n,r,f'}$ whenever $f/f' \in (K^\times)^{p^{r+1}-1}$ has been proven already. Conversely, suppose $H_{n,r,f} \cong H_{n,r,f'}$. Then

$$H_{n,r,f} \otimes K^{p^{-\infty}} \cong H_{n,r,f'} \otimes K^{p^{-\infty}},$$

of course, and, by [6, Sec. 3],

$$f/f' \in \left(\left(K^{p^{-\infty}}\right)^\times\right)^{p^{r+1}-1}.$$

Thus, the equation

$$x^{p^{r+1}} - \frac{f}{f'}x = 0$$

has a solution in $K^{p^{-\infty}}$. If g is such a solution, then $K(g)$ is a separable extension of K contained in $K^{p^{-\infty}}$. Since $K^{p^{-\infty}}/K$ is purely inseparable we have $g \in K$, hence $f/f' \in (K^\times)^{p^{r+1}-1}$. □

Note the parallel with the result in [6] if we replace β with $\beta^{p^{-1}}$ — of course, if f and f' are elements of k (a perfect field contained in K) these Hopf algebras are defined over k and we expect the isomorphism condition above to hold.

4. Hopf Galois objects

Let $L = K(x)$, $x^{p^n} = b \in K$. If H is the monogenic Hopf algebra with primitive generator, then L is an H-Galois object: this is the Hopf algebra used in the construction of [1], where Chase shows that all modular extensions of K are Hopf Galois objects. The purpose of this section is to show that each of the rank p^n Hopf algebras constructed above can be used to make L a Hopf-Galois object.

Let $H = H_{n,r,f}$ for some choice of $0 < r < n$ and $f \in K^\times$. Define $\alpha(x) \in L \otimes H$ by

$$\alpha(x) = S_d\left(\left(f_d x^{p^{dr}} \otimes 1, \ldots, f_1 x^{p^r} \otimes 1, x \otimes 1\right); \left(1 \otimes f_d t^{p^{dr}}, \ldots, 1 \otimes f_1 t^{p^r}, 1 \otimes t\right)\right).$$

We claim that this can be extended to a K-algebra map $\alpha : L \to L \otimes H$; to establish this it suffices to show $\alpha(b) = (\alpha(x))^{p^n}$. Since exponentiation-by-p

is a K-algebra map,

$$\begin{aligned}\alpha(b) &= \alpha\left(x^{p^n}\right)\\ &= S_d\Bigg(\left(f_d^{p^n}\left(x^{p^{dr}}\right)^{p^n}\otimes 1,\ldots,x^{p^n}\otimes 1\right);\\ &\quad \left(1\otimes f_d^{p^n}\left(t^{p^{dr}}\right)^{p^n},\ldots,1\otimes f_1\left(t^{p^r}\right)^{p^n},1\otimes t^{p^n}\right)\Bigg)\\ &= S_d\left(\left(f_d^{p^n}\left(x^{p^{dr}}\right)^{p^n}\otimes 1,\ldots,x^{p^n}\otimes 1\right);(0,\ldots,0)\right)\\ &= x^{p^n}\otimes 1 = b\otimes 1,\end{aligned}$$

and so α is a well-defined K-algebra map.

Lemma 4.1. *The map α above gives L the structure of a right H-comodule.*

Proof. We need to show

$$\begin{aligned}(1\otimes\Delta)\,\alpha(x) &= (\alpha\otimes 1)\,\alpha(x),\\ \mu\,(1\otimes\varepsilon)\,\alpha(x) &= x.\end{aligned}$$

The first follows immediately from the associativity of S_d. The second computation is similar to the one in Equation (2). □

Proposition 4.2. *Let $\gamma : L\otimes L\to L\otimes H$ be given by*

$$\gamma(a\otimes b) = (a\otimes 1)\,\alpha(b).$$

Then γ is a K-module isomorphism, hence L is an H-Galois object.

Proof. First, notice that since α is a K-algebra map we have that γ preserves multiplication, i.e., $\gamma((a\otimes b)(c\otimes d)) = \gamma(a\otimes b)\,\gamma(c\otimes d)$. Also, γ is an L-module map if we view $L\otimes L$ as an L-module via the first factor since $\gamma(a\otimes b) = (a\otimes 1)\,\gamma(b)$. Since $L\otimes L$ and $L\otimes H$ are both K-vector spaces of dimension p^{2n}, it suffices to show that γ is onto. Now

$$\begin{aligned}\gamma(-x\otimes 1+1\otimes x) &= -(x\otimes 1)\,\alpha(1)+(1\otimes 1)\,\alpha(x)\\ &= -x\otimes 1+S_d\Big(\left(f_d x^{p^{dr}}\otimes 1,\ldots,x\otimes 1\right);\\ &\quad \left(1\otimes f_d t^{p^{dr}},\ldots,1\otimes t\right)\Big)\\ &= -x\otimes 1+x\otimes 1+1\otimes t+t^2\xi\\ &= 1\otimes t+t^2\xi_1\end{aligned}$$

for some $\xi_1\in L\otimes H$. As γ is multiplicative we see that

$$\gamma\left((-x\otimes 1+1\otimes x)^i\right) = 1\otimes t^i+t^{i+1}\xi_i,\ \xi_i\in L\otimes H$$

for $1\le i<p^n$. Thus $\left\{\gamma\left((-x\otimes 1+1\otimes x)^i\right)\right\}$ is an L-linearly independent set, we have $\dim_L \operatorname{Im}\gamma\ge p^n$. As $[L:K]=p^n$ we have $\dim_K \operatorname{Im}\gamma\ge p^{2n}$ so $\operatorname{Im}\gamma = L\otimes H$. □

One will notice many parallels between this theory and the Kummer theory of formal groups construction in, e.g., [2, Sec. 39]. This is to be expected since a smooth resolution for Spec $H_{n,r,f}$ can be easily constructed by adapting the resolution in [7, Sec. 4].

Of course, there are many different descriptions for the same field extension L. Indeed, pick $g \in K^\times$ and let $y = gx$. Then $y^{p^n} = g^{p^n} b \in K$ and so $L = K(y)$. With the coaction above we have

$$\begin{aligned}
\alpha(y) &= \alpha(gx) \\
&= gS_d\left(\left(f_d x^{p^{dr}} \otimes 1, \dots, x \otimes 1\right); \left(1 \otimes f_d t^{p^{dr}}, \dots, 1 \otimes t\right)\right) \\
&= S_d\left(\left(g^{p^{-d}} f_d x^{p^{dr}} \otimes 1, \dots, gx \otimes 1\right); \left(1 \otimes g^{p^{-d}} f_d t^{p^{dr}}, \dots, 1 \otimes gt\right)\right) \\
&= S_d\Big(\left(g_d f_d x^{p^{dr}} \otimes 1, \dots, g_1 f_1 x^{p^r} \otimes 1, gx \otimes 1\right); \\
&\qquad \left(1 \otimes g_d f_d t^{p^{dr}}, \dots, g_1 f_1 u^{p^r} t^{p^r}, 1 \otimes gt\right)\Big)
\end{aligned}$$

where $g_i = g^{p^{-i}-p^{ri}}$ as in the previous section. Thus, since $g_1^p = g^{1-p^{r+1}}$, changing the generator of L in this manner results in the same coaction: $t \in H_{n,r,f}$ acts on x in the same way as $gt \in H_{n,r,fg^{1-p^{r+1}}}$ acts on y, and these two Hopf algebras are isomorphic.

On the other hand, let $x_i = x^i$, $1 \le i \le n-1$, $\gcd(p,i) - 1$. Then $L = K(x) = K(x_i)$, and defining

$$\begin{aligned}
&\alpha_i(x_i) = \\
&S_d\Big(\left(f_d x_i^{p^{dr}} \otimes 1, \dots, f_1 x_i^{p^r} \otimes 1, x_i \otimes 1\right); \left(1 \otimes f_d t^{p^{dr}}, \dots, 1 \otimes f_1 t^{p^r}, 1 \otimes t\right)\Big)
\end{aligned}$$

allows for a coaction of $H_{n,r,f}$ on L; as i varies each resulting coaction is different. This provides $\phi(p^n) = p^{n-1}(p-1)$ different ways to view L as an $H_{n,r,f}$-Galois object. There are certainly many other coactions, for example those found by replacing x with wx for $w \in K[x]^\times$; these will not all be distinct coactions, however.

Remark 4.3. Proposition 3.1 can be used to provide examples of finite field extensions L/K with an infinite number of K-Hopf algebras which L is an H-Galois object. For example, let $K = k(T_1, T_2, \dots)$ and let L be any primitive purely inseparable extension of degree p^2 (or greater). Then $H_{n,r,T_i} \ncong H_{n,r,T_j}$ unless $i = j$.

Both Chase's construction and the Hopf algebras presented here can be considered under one general theory. Indeed, were we to allow $r = n$ and $f = 0$, then $d = 0$ and we recover Chase's Hopf algebra. We have chosen to treat them as separate cases to simplify the question of isomorphic Hopf algebras — clearly, the Hopf algebra "$H_{n,n,f}$" does not depend at all on f.

5. Explicit computations: the case $r = n - 1$

We shall now explicitly describe the action of $H := H^*_{n,r,f}$ on L in the case where $r = n-1$. In this case, $d = 1$, and hence the comultiplication on $H_{n,r,f}$ is

$$\Delta(t) = t \otimes 1 + 1 \otimes t + f \sum_{\ell=1}^{p-1} \frac{1}{\ell!\,(p-\ell)!} t^{p^r \ell} \otimes t^{p^r (p-\ell)}.$$

We view this as a restriction on r, not on n — that is, L/K can be any extension, but we only consider the Hopf algebras with $r = n-1$. This will provide a family of explicit Hopf Galois actions on any purely inseparable extension L/K of degree $p^n,\ n \geq 2$.

As a K-module, H has a basis $\{z_0 = 1, z_1, \ldots, z_{p^n-1}\}$ with $z_i : H \to K$ given by

$$z_j\left(t^i\right) = \delta_{i,j},$$

where $\delta_{i,j}$ is the Kronecker delta. The algebra structure on H is induced from the coalgebra structure on $H_{n,r,f}$; explicitly,

$$z_{j_1} z_{j_2}(h) = \operatorname{mult}\left(z_{j_1} \otimes z_{j_2}\right) \Delta(h). \tag{3}$$

We claim that $\left\{z_p, z_{p^2}, z_{p^3}, \ldots, z_{p^r}\right\}$ generate H as a K-algebra.

We start with a result which will facilitate the study of the algebra structure of H as well as the action of H on L.

Lemma 5.1. *Let*

$$S_f(u,v) = u + v + f \sum_{\ell=1}^{p-1} \frac{1}{\ell!\,(p-\ell)!} u^{p^r \ell} v^{p^r (p-\ell)}.$$

Then, for every positive integer i, $S_f(u,v)^i$ is a K-linear combination of elements of the form

$$u^{i_1 + p^r \ell'} v^{i_2 + p^r \ell''},$$

where $i_1 + i_2 + i_3 = i$; $\ell', \ell'' \geq 0$; and $\ell' + \ell'' = p i_3$.

Proof. We have

$$\begin{aligned} S_f(u,v)^i &= \left(u + v + f \sum_{\ell=1}^{p-1} \frac{1}{\ell!\,(p-\ell)!} u^{p^r \ell} v^{p^r (p-\ell)} \right)^i \\ &= \sum_{i_1+i_2+i_3=i} \binom{i}{i_1, i_2, i_3} \left(u^{i_1} v^{i_2}\right) \left(f \sum_{\ell=1}^{p-1} \frac{1}{\ell!\,(p-\ell)!} u^{p^r \ell} v^{p^r (p-\ell)} \right)^{i_3}. \end{aligned}$$

The last factor in each summand can be expanded as

$$f^{i_3} \sum_{i_{3,1}+\cdots+i_{3,p-1}=i_3} \left(\binom{i_3}{i_{3,1}, \ldots, i_{3,p-1}} \left(\prod_{j=1}^{p-1} \frac{1}{\left(\ell!\,(p-\ell)!\right)^{i_{3,j}}} \right) u^{i_1 + p^r \ell'} v^{i_2 + p^r \ell''} \right).$$

The result follows. □

Next, we consider powers of the z_{p^s}'s.

Lemma 5.2. *For* $0 \leq s \leq r,\ 1 \leq m \leq p-1,\ z_{p^s}^m = m! z_{mp^s}$.

Proof. Clearly, this holds for $m = 1$. Suppose $z_{p^s}^{m-1} = (m-1)! z_{(m-1)p^s}$. By Equation (3) we have

$$\begin{aligned} z_{p^s}^m \left(t^i\right) &= \operatorname{mult}\left(z_{p^s}^{m-1} \otimes z_{p^s}\right) \Delta\left(t^i\right) \\ &= \operatorname{mult}\left(z_{p^s}^{m-1} \otimes z_{p^s}\right) S_f \left(t \otimes 1, 1 \otimes t\right)^i \\ &= \operatorname{mult}\left((m-1)! z_{(m-1)p^s} \otimes z_{p^s}\right) \\ &\qquad \left(t \otimes 1 + 1 \otimes t + f \sum_{\ell=1}^{p-1} \frac{1}{\ell!\,(p-\ell)!} t^{p^r \ell} \otimes t^{p^r (p-\ell)}\right)^i. \end{aligned}$$

By Lemma 5.1, the tensors are of the form

$$t^{i_1 + p^r \ell'} \otimes t^{i_2 + p^r \ell''},$$

with ℓ', ℓ'' as before. Recall that $\ell' + \ell'' = p i_3$. Since $z_{p^s}\left(t^\ell\right) = \delta_{p^s,\ell}$ and $z_{(m-1)p^s}\left(t^\ell\right) = \delta_{(m-1)p^s,i}$, the expression

$$\left(z_{(m-1)p^s} \otimes z_{p^s}\right)\left(t^{i_1 + p^r \ell'} \otimes t^{i_2 + p^r \ell''}\right)$$

is nontrivial only if

$$\begin{aligned} (m-1)\, p^s &= i_1 + p^r \ell' \\ p^s &= i_2 + p^r \ell''. \end{aligned}$$

If we add the two equations together we get

$$m p^s = i_1 + i_2 + p^{r+1} i_3.$$

From this it is clear that $i_3 = 0$, which means $\ell' = \ell'' = 0$ as well. Thus $i_2 = p^s$ and $i_1 = (m-1)\, p^s$, hence $i = m p^s$ and with the help of Lucas' Theorem [3] we get

$$\begin{aligned} z_{p^s}^m \left(t^{mp}\right) &= (m-1)! \binom{m p^s}{(m-1)\, p^s, p^s, 0} \\ &= (m-1)! \binom{m p^s}{p^s} \\ &= (m-1)! m \\ &= m! \end{aligned}$$

Therefore, $z_{p^s}^m = m! z_{mp^s}$. □

Lemma 5.3. *For* $0 \leq s \leq r-1,\ z_{p^s}^p = 0$.

Proof. We have

$$z_{p^s}^p\left(t^i\right) = (p-1)!\,\mathrm{mult}\left(z_{(p-1)p^s}\otimes z_{p^s}\right)\left(\sum_{i_1+i_2+i_3=i}\binom{i}{i_1,i_2,i_3}\left(t^{i_1}\otimes t^{i_2}\right)\right.$$
$$\left.\cdot\left(f\sum_{\ell=1}^{p-1}\frac{1}{\ell!\,(p-\ell)!}t^{p^r\ell}\otimes t^{p^r(p-\ell)}\right)^{i_3}\right).$$

If $\left(z_{(p-1)p}\otimes z_p\right)\left(t^{i_1+p^r\ell'}\otimes t^{i_2+p^r\ell''}\right)$ is nontrivial then

$$(p-1)\,p^s = i_1+p^r\ell'$$
$$p^s = i_2+p^r\ell''.$$

Again, $i_3=0$, so $i_2=p^s$ and $i_1=(p-1)\,p^s$, hence $i=p^{s+1}$. But then

$$\begin{aligned} z_{p^s}^p\left(t^{p^{s+1}}\right) &= (p-1)!\binom{p^{s+1}}{(p-1)\,p^s,p^s,0}\\ &= -\binom{p^{s+1}}{p^s}\\ &= 0. \end{aligned}$$

So $z_{p^s}^p=0$. □

Remark 5.4. While not part of the generating set we are constructing, notice that the above results show $z_1^m = m!z_m$ and $z_1^p=0$.

The behavior is slightly different for p^r.

Lemma 5.5. *We have $z_{p^r}^p = fz_1$ and $z_{p^r}^{p^2}=0$.*

Proof. If the expression $\left(z_{(p-1)p^r}\otimes z_{p^r}\right)\left(t^{i_1+p^r\ell'}\otimes t^{i_2+p^r\ell''}\right)$ in the expansion of $z_{p^r}^p\left(t^i\right)$is nontrivial then

$$(p-1)\,p^r = i_1+p^r\ell'$$
$$p^r = i_2+p^r\ell''.$$

If $i_3=0$ then $i_2=p^r$, $i_1=(p-1)\,p^r$ and $i=p^{r+1}$; however, $i<p^{r+1}=p^n$ so this cannot occur. Thus $i_3=1$, $\ell^{'}=p-1$, $\ell''=1$ (both of these can occur only by setting $i_{3,j}=\delta_{j,p-1}$), $i_2=0$, and $i_1=0$. Hence, $i=1$ and

$$z_{p^r}^p(t) = (p-1)!\binom{1}{0,0,1}f\frac{1}{(p-1)!\,(p-(p-1))!} = f.$$

Therefore, $z_{p^r}^p=fz_1$. That $z_{p^r}^{p^2}=0$ follows immediately. □

From the results above, we can deduce that $\{z_{p^s}:1\le s\le r\}$ generate H as a K-algebra.

The coalgebra structure on H is induced from the multiplication on $H_{n,r,f}$ and is much more straightforward. For all $h \in H$, when we apply the comultiplication Δ we get a K-linear map $H_{n,r,f} \otimes H_{n,r,f} \to K$ given by

$$\Delta(h)(a \otimes b) = h(ab).$$

Thus,

$$\Delta(z_j)\left(t^{i_1} \otimes t^{i_2}\right) = z_j\left(t^{i_1+i_2}\right) = \delta_{j,i_1+i_2}$$

and so

$$\Delta(z_j) = \sum_{i=0}^{j} z_{j-i} \otimes z_i.$$

Note that this is true for all j, not just the powers of p.

We summarize.

Proposition 5.6. *The Hopf algebra H above is*

$$H = K\left[z_p, z_{p^2}, \ldots, z_{p^r}\right] / \left(z_p^p, z_{p^2}^p, \ldots, z_{p^{r-1}}^p, z_{p^r}^{p^2}\right)$$

$$\Delta(z_{p^s}) = \sum_{i=0}^{p^s} z_{p^s-i} \otimes z_i.$$

Of course, it is possible to write $\Delta(z_{p^s})$ solely in terms of $z_p, \ldots, z_{p^r}$, but that is not needed for our purposes.

We will now describe the Hopf Galois action of H on L. The K-algebra map $\alpha : L \to L \otimes H_{n,r,f}$ is given by

$$\alpha(x) = x \otimes 1 + 1 \otimes t + f \sum_{\ell=1}^{p-1} \frac{1}{\ell!\,(p-\ell)!} x^{p^r \ell} \otimes t^{p^r(p-\ell)}.$$

This gives L the structure of an $H_{n,r,f}$-comodule — in fact it makes L an $H_{n,r,f}$-Galois object. Here, we compute the induced action of H on L which makes L/K an H-Galois extension.

Generally, if A is a K-Hopf algebra such that L is an A-Galois object, then A^* acts on L by

$$h(y) = \mathrm{mult}(1 \otimes h)\,\alpha(y),\ h \in A^*, y \in L. \tag{4}$$

Here, it suffices to compute $z_{p^s}\left(x^i\right)$ for $1 \le s \le r$, $1 \le i \le p^n - 1$, however it will also be useful to compute $z_j\left(x^i\right)$ for some choices of j which are not powers of p. Notice that we use $z_j(-)$ in two different contexts: one to describe z_j as a map $H_{n,r,f} \to K$, the other to describe how z_j acts on L.

The first result handles the case $i = 1$.

Lemma 5.7. *We have*

$$z_0(x) = x,\ z_1(x) = 1,\ z_{p^r}(x) = -f x^{p^r(p-1)}.$$

For $1 \le j \le p^r - 1$, $z_j(x) = 0$.

Proof. Applying Equation 4 to $h = z_j$, $y = x$ gives

$$z_j(x) = xz_j(1) + z_j(t) + f\sum_{\ell=1}^{p-1} \frac{1}{\ell!\,(p-\ell)!} x^{p^r\ell} z_j\left(t^{p^r(p-\ell)}\right),$$

from which the result follows. □

The second result handles the cases where i is a nontrivial power of p.

Lemma 5.8. *For $1 \leq m \leq r$ we have*

$$z_0\left(x^{p^m}\right) = x^{p^m},\ z_{p^m}\left(x^{p^m}\right) = 1.$$

For all other choices of j, $z_j\left(x^{p^m}\right) = 0$.

Proof. The computations are facilitated by observing that $\alpha\left(x^{p^m}\right) = x^{p^m} \otimes 1 + 1 \otimes t^{p^m}$. Indeed,

$$\begin{aligned}
\alpha\left(x^{p^m}\right) &= \alpha(x)^{p^m} \\
&= \left(x \otimes 1 + 1 \otimes t + f\sum_{\ell=1}^{p-1} \frac{1}{\ell!\,(p-\ell)!} x^{p^r\ell} \otimes t^{p^r(p-\ell)}\right)^{p^m} \\
&= x^{p^m} \otimes 1 + 1 \otimes t^{p^m} + f\sum_{\ell=1}^{p-1} \frac{1}{\ell!\,(p-\ell)!} x^{p^{r+m}\ell} \otimes t^{p^{r+m}(p-\ell)} \\
&= x^{p^m} \otimes 1 + 1 \otimes t^{p^m}
\end{aligned}$$

since $r + m \geq r + 1 = n$. Now for $0 \leq j \leq p^n - 1$ we have

$$z_j\left(x^{p^m}\right) = x^{p^m} z_j(1) + z_j\left(t^{p^m}\right),$$

from which the result follows. □

Next, we have

Theorem 5.9. *Let $H = H^*_{n,r,f}$ be as in Proposition 5.6, that is,*

$$H = K\left[z_p, z_{p^2}, \ldots, z_{p^r}\right] / \left(z_p^p, z_{p^2}^p, \ldots, z_{p^{r-1}}^p, z_{p^r}^{p^2}\right)$$

$$\Delta(z_{p^s}) = \sum_{i=0}^{p^s} z_{p^s-i} \otimes z_i.$$

For $0 \leq i \leq p^n - 1$, write

$$i = \sum_{\ell=0}^{r} i_{(\ell)} p^\ell,\ \textit{where } 0 \leq i_{(\ell)} \leq p-1.$$

Then, for $0 \leq s \leq r-1$ we have

$$z_{p^s}\left(x^i\right) = i_{(s)} x^{i-p^s}.$$

Additionally,

$$z_{p^r}\left(x^i\right) = i_{(r)} x^{i-p^r} - if x^{p^r(p-1)+i-1}.$$

Remark 5.10. Note that if $i < p^s < p^r$ then $z_{p^s}\left(x^i\right) = 0$, and if $i < p^r$ then $z_{p^r}\left(x^i\right) = -ifx^{p^r(p-1)+i-1}$.

Proof. We have

$$\begin{aligned} z_{p^s}\left(x^i\right) &= \operatorname{mult}\left(1 \otimes z_{p^s}\right)\alpha\left(x^i\right) \\ &= \operatorname{mult}\left(1 \otimes z_{p^s}\right)S_f\left(x \otimes 1, 1 \otimes t\right)^i \\ &= \operatorname{mult}\left(1 \otimes z_{p^s}\right)\left(x \otimes 1 + 1 \otimes t + f\sum_{\ell=1}^{p-1}\frac{1}{\ell!\,(p-\ell)!}x^{p^r\ell} \otimes t^{p^r(p-\ell)}\right)^i \\ &= \operatorname{mult}\left(1 \otimes z_{p^s}\right)\sum_{i_1+i_2+i_3=i}\binom{i}{i_1, i_2, i_3}\left(x^{i_1} \otimes t^{i_2}\right) \\ &\quad \cdot \left(f\sum_{\ell=1}^{p-1}\frac{1}{\ell!\,(p-\ell)!}x^{p^r\ell} \otimes t^{p^r(p-\ell)}\right)^{i_3}. \end{aligned}$$

After expanding, the tensors are of the form $x^{i_1+p^r\ell'} \otimes t^{i_2+p^r\ell''}$, ℓ', ℓ'' as before. Applying $1 \otimes z_{p^s}$ to this expression will give 0 unless

$$p^s = i_2 + p^r\ell''. \tag{5}$$

Assume first that $s < r$. Since $p^r > p^s$ we see that $i_3 = 0$ and $i_2 = p^s$. Thus $i_1 = i - p^s$ and we get

$$\begin{aligned} z_{p^s}\left(x^i\right) &= \binom{i}{i-p^s, p^s, 0}x^{i-p^s}z_{p^s}\left(t^{p^s}\right) \\ &= \binom{i}{p^s}x^{i-p^s} \\ &= i_{(s)}x^{i-p^s}, \end{aligned}$$

as desired.

Now we consider the case $s = r$. Then $i_3 = 0$, $i_2 = p^r$, $i_1 = i - p^r$ certainly satisfies Equation 5. However, we get an additional solution to this equation, namely $i_3 = 1$, $\ell = p-1$, $i_2 = 0$, $i_1 = i-1$. Thus

$$\begin{aligned} z_{p^r}\left(x^i\right) &= \binom{i}{i-p^r, p^r, 0}x^{i-p^r}z_{p^r}\left(t^{p^r}\right) \\ &\quad + \binom{i}{i-1, 0, 1}x^{i-1}f\frac{1}{(p-1)!\,(p-(p-1))!}x^{p^r(p-1)}z_{p^r}\left(t^{p^r}\right) \\ &= i_{(r)}x^{i-p^r} - ifx^{p^r(p-1)+i-1}. \end{aligned}$$

□

The results above do not generalize easily to the case $n > r+1$. Certainly, if $2r < n$ then the comultiplication on $H_{n,r,f}$ (and its coaction on L) becomes much more complicated, making the computations of the algebra structure (and the action) of its dual much more involved as well. If $r+1 < n \leq 2r$, computation of the algebra structure of $H^*_{n,r,f}$ is somewhat more complex

than the case considered here — in particular, $z_{p^r}^p \neq f z_1$ — but, as a future paper [8] will show, it is possible to show that $H_{n,r,f}^*$ is generated as a K-module by $\left\{\prod_{s=0}^{n-1} z_{p^s}^{j_s} : 0 \leq j_s \leq p-1\right\}$, and much of its action on L can be made explicit.

6. A note on modular extensions

While the focus of this work is primitive purely inseparable extensions, it should be pointed out that the constructions here can be adapted easily to general modular extensions. The following should be clear.

Proposition 6.1. *Let L/K be modular, $L \cong L_1 \otimes \cdots \otimes L_s$ with L_i/K primitive of degree p^{n_i}, $n_i \geq 2$, $1 \leq i \leq s$. For each i, pick $0 < r_i < n_i$ and $f_i \in K^\times$. Set*

$$H = H_{n_1,r_1,f_1} \otimes \cdots \otimes H_{n_s,r_s,f_s}.$$

Then L is an H-Galois object.

Thus, the constructions in the previous sections show that any modular extension of exponent at least 2 can be equipped with numerous Hopf Galois structures. However, it is not the case that all (local-local) Hopf Galois structures on modular extensions have been exhibited here, as the following example shows.

Example 6.2. Let $K = \mathbb{F}_p(T_1, T_2)$. Let $L = K(x, y)$ with $x^{p^2} = T_1$, $y^{p^2} = T_2$. Then L/K is modular. Let $H = K(t, u) / \left(t^{p^2}, u^{p^2}\right)$, and define $\Delta : H \to H \otimes H$ by

$$\Delta(t) = S_3\left((u^p \otimes 1, t^p \otimes 1, u \otimes 1, t \otimes 1); (1 \otimes u^p, 1 \otimes t^p, 1 \otimes u, 1 \otimes t)\right)$$
$$\Delta(u) = S_2\left((u^p \otimes 1, t^p \otimes 1, u \otimes 1); (1 \otimes u^p, 1 \otimes t^p, 1 \otimes u)\right).$$

Along with the counit ε given by $\varepsilon(t) = \varepsilon(u) = 0$ and antipode $\lambda(t) = -t, \lambda(u) = -u$, this gives H the structure of a K-Hopf algebra which is not monogenic: checking that the Hopf algebra axioms hold is straightforward. Define $\alpha : L \to L \otimes H$ by

$$\alpha(x) = S_3\left((y^p \otimes 1, x^p \otimes 1, y \otimes 1, x \otimes 1); (1 \otimes u^p, 1 \otimes t^p, 1 \otimes u, 1 \otimes t)\right)$$
$$\alpha(y) = S_2\left((y^p \otimes 1, x^p \otimes 1, y \otimes 1); (1 \otimes u^p, 1 \otimes t^p, 1 \otimes u)\right).$$

Then L is an H-Galois object. The proof is almost identical to the proofs of Lemma 4.1 and Proposition 4.2.

In fact, this example seems to suggest that the biggest obstacle to a modular extension L being an H-Galois object is the algebra structure of H; the coalgebra structure seems to naturally give a coaction. If L is an H-Galois object, then $L \otimes L \cong L \otimes H$. Also, $L \otimes L$ is a truncated polynomial algebra: in the simple, degree p^n case $L = K(x)$, clearly we have $L(u) / \left(u^{p^n}\right) \cong L \otimes L$ via $u \mapsto 1 \otimes x - x \otimes 1$. Thus, for a given modular

extension L/K, the problem appears to be reduced to finding the Hopf algebra structures on the truncated polynomial algebra $L \otimes L$. We have not found a local-local Hopf algebra of the proper type (as an algebra) which does not give L the structure of an H-Galois object.

References

[1] Chase, Stephen U. Infinitesimal group scheme actions on finite field extensions. *Amer. J. Math.* **98** (1976), no. 2 441–480. MR0424773 (54 #12731), Zbl 0374.12014.

[2] Childs, Lindsay N. Taming wild extensions: Hopf algebras and local Galois module theory. Mathematical Surveys and Monographs, 80. *American Mathematical Society, Providence, RI*, 2000. viii+215 pp. ISBN: 0-8218-2131-8. MR1767499 (2001e:11116), Zbl 0944.11038.

[3] Fine, N. J. Binomial coefficients modulo a prime. *Amer. Math. Monthly* **54** (1947), 589–592. MR0023257 (9,331b), Zbl 0030.11102.

[4] Greither, Cornelius; Pareigis, Bodo. Hopf Galois theory for separable field extensions. *J. Algebra* **106** (1987), no. 1 239–258. MR878476 (88i:12006), Zbl 0615.12026, doi: 10.1016/0021-8693(87)90029-9.

[5] Jacobson, Nathan. Lectures in abstract algebra, III. Theory of fields and Galois theory. Second corrected printing. Graduate Texts in Mathematics, 32. *Springer-Verlag, New York-Heidelberg*, 1975. xi+323 pp. MR0392906 (52 #13719), Zbl 0455.12001.

[6] Koch, Alan. Monogenic bialgebras over finite fields and rings of Witt vectors. *J. Pure Appl. Algebra* **163** (2001), no. 2, 193–207. MR1846661 (2002g:14067), Zbl 0988.16026, doi: 10.1016/S0022-4049(00)00163-8.

[7] Koch, Alan. Monogenic Hopf algebras and local Galois module theory. *J. Algebra* **264** (2003), no. 2, 408–419. MR1981413 (2004d:16068), Zbl 1028.16018, doi: 10.1016/S0021-8693(03)00176-5.

[8] Koch, Alan. Scaffolds and integral Hopf Galois module structure on purely inseparable extensions. Preprint, (2014). arXiv:1405.7608.

[9] Waterhouse, William C. Introduction to affine group schemes. Graduate Texts in Mathematics, 66. *Springer-Verlag, New York-Berlin*, 1979. xi+164 pp. ISBN: 0-387-90421-2. MR547117 (82e:14003), Zbl 0442.14017, doi: 10.1007/978-1-4612-6217-6.

Department of Mathematics, Agnes Scott College, 141 E. College Ave., Decatur, GA 30030, USA
akoch@agnesscott.edu

This paper is available via http://nyjm.albany.edu/j/2014/20-39.html.