Illinois Journal of Mathematics
Volume 48, Number 3, Fall 2004, Pages 923–940
S 0019-2082

DUALS OF FORMAL GROUP HOPF ORDERS IN CYCLIC GROUPS

LINDSAY N. CHILDS AND ROBERT G. UNDERWOOD

Abstract. Let p be a prime number, K be a finite extension of the p-adic rational numbers containing a primitive p^nth root of unity, R be the valuation ring of K and G be the cyclic group of order p^n. We define triangular Hopf orders over R in KG, and show that there exist triangular Hopf orders with $n(n+1)/2$ parameters by showing that the linear duals of "sufficiently p-adic" formal group Hopf orders are triangular.

0. Introduction

This paper is part of a program to determine the structure of commutative, cocommutative finite Hopf algebras over valuation rings of local fields (finite extensions of the p-adic rationals). (The problem is the same as that of describing finite abelian group schemes over valuation rings of local fields.) If the rank of the Hopf algebra is prime to p, then the problem reduces to descent theory, since any such Hopf algebra is a form of the group ring of a finite group. But for Hopf algebras of rank n, where n is a power of p, even the case $n = p$ is nontrivial.

The first general description of Hopf algebras over valuation rings of local fields was that of Tate and Oort [TO70] for Hopf algebras of rank p, in 1970. The Hopf algebras involve a single parameter b of R. Their classification was extended in 1974 by Raynaud [Ra74] to a construction of certain Hopf orders in KG, G elementary abelian of order p^n. In both cases the corresponding finite group schemes admit an action by the multiplicative group of the finite field of order p^n, which allows an eigenspace decomposition of the group scheme, leading to the classification. Hopf orders whose finite group schemes admit such an action are known as Raynaud orders.

Larson [La76] described a construction of Hopf orders in KG for any group G, using the concept of group valuation. For G of order p this construction

Received November 12, 2003; received in final form January 27, 2004.
2000 *Mathematics Subject Classification.* Primary 11S31, 14L05, 16W30.

yields all Hopf orders in KG. These orders have subsequently become known as Larson orders.

Greither [Gr92] and Byott [By93] classified Hopf orders in KG, G of order p^2. Their classification showed that Larson orders form a proper subset of all Hopf orders in KG: for order p^2, Larson orders involve two valuation parameters, while Greither orders involve an additional unit parameter u. Greither determined the allowable valuations of $u-1$ and determined for which valuations the corresponding Hopf order is realizable, that is, is the associated order of the valuation ring of some Galois extension L/K of local fields with cyclic Galois group G of order p^2. Greither's classification assumed a p-adic condition on the valuation parameters, following Larson; his classification was extended by Underwood to arbitrary orders in KG [Un94], and by Childs (partially) [Ch95] and Byott (fully) [By02] to Hopf orders in arbitrary abelian K-Hopf algebras of rank p^2.

For rank p^n, $n > 2$, only partial results are known. Childs and Sauerberg [CS98] gave a construction of Hopf orders in KG, G elementary abelian of order p^n, using polynomial formal groups. Greither and Childs [GC98] extended Greither's construction of Hopf algebras of rank p^2 to obtain Hopf orders in KG, G elementary abelian of order p^n. Both of these constructions obtained for the first time Raynaud orders as iterated extensions of Hopf orders of smaller rank. Greither and Childs' construction was extended by Smith [Sm97]. All three of these constructions obtained Hopf orders that had n valuation parameters and $n(n-1)/2$ unit parameters. When the unit parameters are trivial, the resulting Hopf orders are Larson.

Underwood [Un96] extended Greither's cohomological methods in the p^2 case to construct Hopf orders of rank p^3 as extensions of a Hopf algebra of rank p by a Hopf algebra of rank p^2 that is the dual of a Greither order. His Hopf orders involve three valuation parameters and two unit parameters. In [UC05] we called these *cohomological Hopf orders*.

In [CU03] the authors gave a new construction of Hopf orders in KG, G cyclic of order p^n, using polynomial formal groups. We called the Hopf orders so constructed *formal group Hopf orders*. When G is cyclic of order p^3, this construction yields Hopf orders with six parameters that are not included in the class of cohomological Hopf orders constructed in [Un96]. However, these Hopf orders are not realizable if $n > 1$, hence the class of Hopf orders constructed by the polynomial formal group method cannot include all Hopf orders.

In [UC05] the authors specialized to G cyclic of order p^3. We extended the construction of [Un96] to obtain what we called *triangular Hopf orders* in KG. Cohomological Hopf orders are triangular. One of the main results of [UC05] was that the dual of any formal group Hopf order in KG, G cyclic of order p^3, is triangular.

Suppose henceforth that G is cyclic of order p^n. The purpose of this paper is to introduce triangular Hopf orders in KG. Showing that a triangular Hopf order is in fact a Hopf order (that is, is an R-algebra that as an R-module is free of rank p^n over R and is closed under the comultiplication in KG) is in general difficult. Our main result generalizes the duality result for $n = 3$ in [UC05], namely, that if we impose a suitable p-adic condition on the valuation parameters of the formal group Hopf orders in KG constructed in [CU03], then their duals are triangular. This result implies the existence for all $n > 0$ of triangular Hopf orders in KG with $n(n-1)/2$ unit parameters.

The first author would like to thank Auburn University, Auburn University Montgomery and Union College for their hospitality during this research.

1. Triangular Hopf orders

Let p be a prime number and let the field K be a finite extension of $\mathbb{Q}_p$. Let $\mathrm{ord}(a)$ be the valuation of a in K, normalized so that $\mathrm{ord}(\pi) = 1$, where π is a parameter for K, and let R be the valuation ring of K. Let C_{p^n} denote the cyclic group of order p^n generated by g and suppose K contains a primitive p^nth root of unity ζ_n, with $\zeta_1 = \zeta_n^{p^{n-1}}$ a primitive pth root of unity. Let $e' = e/(p-1)$, where $e = \mathrm{ord}(p)$ is the absolute ramification index of $K/\mathbb{Q}_p$. For an integer i, $0 \le i \le e'$, set $i' = e' - i$.

In [UC05] the authors defined triangular Hopf orders in KC_{p^3} by analogy with the Hopf orders defined in KC_p^n in [GC98]. We begin by defining triangular Hopf orders in KC_{p^n} for all $n > 0$, as follows.

For $0 \le s \le p^n - 1$ let $e_s^{(n)}$ be the primitive idempotent of $K\langle g\rangle$ defined by

$$e_s^{(n)} = \frac{1}{p^n}\sum_{k=0}^{p^n-1} \zeta_n^{-sk} g^k.$$

Write s p-adically, $s = r_0 + pr_1 + p^2r_2 + \cdots + p^{n-1}r_{n-1}$, and for $1 \le k \le n-1$ let

$$a_x^{(k)} = \sum_{r_0,\ldots,r_{n-1}=0}^{p-1} x^{r_{k-1}} e_s^{(n)}.$$

Then a Hopf order H in KG is *triangular* if H has the form

$$H = H(i_n', \ldots, i_1', x_{n-1,1}, x_{n-2,1}, x_{n-2,2}, \ldots, x_{1,n-1}) = R[b_n, b_{n-1}, \ldots, b_1],$$

where

$$b_n = \frac{g^{p^{n-1}} - 1}{\pi^{i'_n}},$$
$$b_{n-1} = \frac{a^{(1)}_{x_{n-1,1}} g^{p^{n-2}} - 1}{\pi^{i'_{n-1}}},$$
$$\dots$$
$$b_1 = \frac{a^{(1)}_{x_{1,1}} a^{(2)}_{x_{1,2}} \cdot \dots \cdot a^{(n-1)}_{x_{1,n-1}} g - 1}{\pi^{i'_1}},$$

where the $x_{\ell,m}$ are units of R (the unit parameters), and $i_1, \dots, i_n$ are non-negative integers (the valuation parameters). (The terminology "triangular" stems from the idea that the parameters may be laid out in a lower triangular matrix. There is no known connection with the terminology "quasi-triangular" in quantum group theory.)

If all the unit parameters are equal to 1 and the valuation parameters satisfy the p-adic condition $i_k \geq pi_{k+1}$ for all k, then $H = H(i_1, \dots, i_n)$ is a Larson order.

These algebras extend known constructions in KC_{p^2} and KC_{p^3} as follows.

For $n = 2$, let $G = \langle g \rangle$ be cyclic of order p^2. For $0 \leq s \leq p-1$ let $e^{(1)}_s$ be the primitive idempotents of $K\langle g^p \rangle = KC_p$ defined by

$$e^{(1)}_s = \frac{1}{p} \sum_{k=0}^{p-1} \zeta_1^{-sk} g^{pk},$$

and for u in R let

$$a_u = \sum_{r=0}^{p-1} u^r e^{(1)}_r.$$

Then every R-Hopf order in KG_{p^2} has the form

$$H = R\left[\frac{g^p - 1}{\pi^{i_1}}, \frac{a_u g - 1}{\pi^{i_2}}\right]$$

by [Gr92] and [Un94]. The parameters i_1, i_2 are the valuation parameters, and determine the discriminant of H; the parameter u is a unit parameter: H is a Hopf order if $u - 1$ has valuation $\geq \max\{i'_1 + i_2/p, i'_1/p + i_2\}$, and H is visibly Larson if $u = 1$ and is demonstrably Larson if $\mathrm{ord}(u-1) \geq i'_1 + i_2$.

One sees easily that

$$e^{(1)}_{r_0} = \sum_{r_1=0}^{p-1} e^{(2)}_{r_0 + pr_1},$$

and so

$$a_u = a^{(1)}_u = \sum_{r_0, r_1 = 0}^{p-1} u^{r_0} e^{(2)}_{r_0 + pr_1}.$$

Thus all Hopf orders in KG_{p^2} are triangular.

For $n = 3$, let $e^{(2)}_{r_0+pr_1}$, $r_0, r_1 = 0, \ldots, p-1$, be the primitive idempotents of $K\langle g^p\rangle = KC_{p^2}$. For u, v, w units of R, define

$$b_w = \sum_{r_0,r_1=0}^{p-1} w^{r_1} e^{(2)}_{r_0+pr_1},$$

$$a_v = \sum_{r_0,r_1=0}^{p-1} v^{r_0} e^{(2)}_{r_0+pr_1},$$

$$a_u = \sum_{r_0,r_1=0}^{p-1} u^{r_0} e^{(2)}_{r_0+pr_1}.$$

In [UC05, §1] we defined Hopf orders in KC_{p^3} of the form

$$H(i_1, i_2, i_3, u, v, w) = R\left[\frac{g^{p^2}-1}{\pi^{i_1}}, \frac{a_u g^p - 1}{\pi^{i_2}}, \frac{a_v b_w g - 1}{\pi^{i_3}}\right],$$

where

$$a_v b_w = \sum_{r_0,r_1=0}^{p-1} v^{r_0} w^{r_1} e^{(2)}_{r_0+pr_1}.$$

One sees easily that

$$e^{(2)}_{r_0+pr_1} = \sum_{r_2=0}^{p-1} e^{(3)}_{r_0+pr_1+p^2r_2};$$

thus $a_u = a^{(1)}_u$, $a_v = a^{(1)}_v$, and $b_w = a^{(2)}_w$, and so these Hopf orders are triangular. Here the i_j are valuation parameters and u, v, w are unit parameters. If $u = v = w = 1$ and the valuation parameters i_1, i_2, i_3 satisfy a p-adic condition, then $H(i_1, i_2, i_3, u, v, w)$ is a Larson order. We have found sets of sufficient conditions on the parameters for these triangular algebras $H(i_1, i_2, i_3, u, v, w)$ to be Hopf orders; cf. [UC05, Theorem 1.7, Proposition 1.8, Theorem 3.7]. However those conditions are complicated, and in contrast to the case for $n = 2$ there exist Hopf orders in KG with $n = 3$ that are not triangular; cf. [UC05, Theorem 4.3] or [CU03, Theorem 4.2].

For $n > 3$ the only triangular Hopf orders previously known to exist were Larson orders, though for large n one can construct non-Larson triangular orders by starting with some Larson orders in KG and simply "pushing up" some non-Larson orders one already knows from the case $n = 2$. These triangular orders in KG, $n > 3$, however, will have only 1 nontrivial unit parameter. Theorem 2.2, below, shows the existence of triangular Hopf orders with $n(n-1)/2$ nontrivial unit parameters.

2. Formal group Hopf orders

In [CU03], the authors constructed Hopf orders over R in KG using n-dimensional degree 2 polynomial formal groups. The construction uses formal groups $\mathcal{F}_\Theta$ obtained by conjugating the n-dimensional multiplicative formal group $\mathbb{G}_m^n$ by suitable $n \times n$ lower triangular matrices Θ with entries in R. The Hopf orders H_Θ in KG represent the kernels of certain isogenies on $\mathcal{F}_\Theta$. We call these *formal group Hopf orders*.

The algebra structure of H_Θ is determined from Θ as follows. Let $U = (u_{i,j})$ denote the lower triangular matrix which is the inverse of Θ. Then (cf. [CS98, p. 71])

$$H_\Theta = R[z_1, z_2, \ldots, z_n],$$

where

$$\begin{aligned} z_1 &= u_{1,1}(g^{p^{n-1}} - 1), \\ z_2 &= u_{2,1}(g^{p^{n-1}} - 1) + u_{2,2}(g^{p^{n-2}} - 1), \\ &\ \vdots \\ z_n &= u_{n,1}(g^{p^{n-1}} - 1) + \cdots + u_{n,n}(g - 1). \end{aligned}$$

In [CU03] we obtained the following theorem:

THEOREM 2.1 ([CU03, Theorem 2.1]). *Suppose $\Theta = (\theta_{i,j})$ is an $n \times n$ lower triangular matrix with entries in R with the following properties:*

- *The diagonal entries $\theta_{\ell,\ell}$ are non-zero.*
- *There exists q with $0 < q < (p-1)/(2p-1)(< 1/2)$, so that the non-zero entries $\theta_{\ell,j}$ in the ℓth row have valuations $\operatorname{ord}(\theta_{\ell,j})$ satisfying*

$$\operatorname{ord}(\theta_{\ell,\ell}) > \operatorname{ord}(\theta_{\ell,i}) \geq (1-q)\operatorname{ord}(\theta_{\ell,\ell})(> \frac{1}{2}\operatorname{ord}(\theta_{\ell,\ell})).$$

- *The diagonal entries $\theta_{\ell,\ell}$ satisfy a kind of "p-adic" condition,*

$$\operatorname{ord}(\theta_{\ell,\ell}) \geq d\operatorname{ord}(\theta_{\ell+1,\ell+1})$$

  for $\ell \geq 1$, where

$$d \geq \frac{p}{1-q} + \frac{q}{1 - \frac{1-q}{p}}.$$

- *The entry $\theta_{1,1}$ has valuation not too close to e'; in particular,*

$$\operatorname{ord}(\theta_{1,1}) < \left(\frac{p-1}{p}\right)\left(\frac{d-1}{d-1+q}\right)e'.$$

Then Θ gives rise to an R-Hopf order H_Θ in KC_{p^n}.

We can assume that the diagonal entries $\theta_{\ell,\ell}$ are pure powers of π:

$$\theta_{\ell,\ell} = \pi^{i_\ell}.$$

Then the i_ℓ are the "valuation parameters" of H_Θ, in the sense that the rank p subquotients of H_Θ, namely, the orders in $K\langle\sigma_\ell\rangle$ where $\sigma_\ell = g^{p^{n-\ell}} + \langle g^{p^{n-\ell+1}}\rangle$, are the rank p Larson orders $H(i_\ell) = R[(\sigma_\ell - 1)/\pi^{i_\ell}]$ and hence the discriminant of H_Θ is completely determined by the i_ℓ (cf. [Ch00, (22.17)]).

Our main result, stated in the following theorem, is that by assuming a stronger p-adic condition on the diagonal entries of Θ we can identify the dual of H_Θ as a triangular Hopf order J. One consequence of this identification is that we don't need to know in advance that J is anything more than an R-algebra, for once we show that J is the dual of H_Θ, J must be a Hopf order since the dual of H_Θ is. In this way we obtain triangular Hopf orders in KC_{p^n} for all n.

THEOREM 2.2. *Let $H = H_\Theta$ be as in Theorem 2.1, and suppose $i_{s-1} \geq 2npi_s$ for all $s > 1$. Then the dual of H_Θ is triangular.*

It is easy to see that the p-adic condition in Theorem 2.2 implies that in Theorem 2.1.

Proof. Throughout this proof H^* will denote the linear dual of the Hopf order H. Let $\hat{G} = \langle\gamma\rangle$ be the character group of G, where $\langle\gamma, g\rangle = \zeta_n$.

When $n = 1$, H is the Larson order $H(i_1) = R[(g-1)/\pi^{i_1}]$ and $H(i_1)^*$ is $H(i'_1) = R[(\gamma - 1)/\pi^{i'_1}]$ (see [Ch00, (21.2)]), so the result is true when $n = 1$.

To prove the result for $n \geq 2$, the triangular dual of H will be constructed inductively, adding one generator at each inductive step. For the induction hypothesis we assume that the rank p^{n-1} sub-Hopf order $H^* \cap K\langle\gamma^p\rangle$ of H^* is triangular. Using this, we then find a new generator, which when adjoined to the sub-Hopf order results in an R-algebra of triangular form which is contained in the dual of H. A discriminant argument then shows that this triangular R-algebra is the dual of H.

Let $\langle -, -\rangle$ be the duality pairing: $K\hat{G} \times KG \to K$, such that $\langle\gamma, g\rangle = \zeta_n$. Let Θ_2 be the $n-1 \times n-1$ matrix obtained from Θ by omitting the first row and column. Then the image of H_Θ under the quotient map on KG defined by sending $g^{p^{n-1}}$ to 1 is H_{Θ_2}. Let J_2 be the linear dual of H_{Θ_2}. Note that J_2 is a rank p^{n-1} Hopf order with $J_2 = H^* \cap K\langle\gamma^p\rangle$. We assume that J_2 is triangular of the form

$$J_2 = R[b_n, b_{n-1}, \ldots, b_2],$$

where

$$b_n = \frac{\gamma^{p^{n-1}} - 1}{\pi^{i'_n}},$$

$$b_{n-1} = \frac{a^{(1)}_{x_{n-1,1}}\gamma^{p^{n-2}} - 1}{\pi^{i'_{n-1}}},$$

$$\cdots$$

$$b_2 = \frac{a^{(1)}_{x_{2,1}} a^{(2)}_{x_{2,2}} \cdot \cdots \cdot a^{(n-2)}_{x_{2,n-2}}\gamma^{p} - 1}{\pi^{i'_2}},$$

where the $x_{\ell,m}$ are units of R (the unit parameters), and $i'_n, \ldots, i'_2$ are non-negative integers (the valuation parameters). Recall that $i' = e' - i$ for any integer i, $0 \le i \le e'$.

J_2 is a sub-Hopf order of H^* with

$$\langle J_2, H\rangle = \langle J_2, H_{\Theta_2}\rangle_2 \subset R,$$

where $\langle -, -\rangle_2$ denotes the duality pairing: $K\hat{C}_{p^{n-1}} \times KC_{p^{n-1}} \to K$.

Now put

$$b_1 = \frac{a^{(1)}_{x_{1,1}} a^{(2)}_{x_{1,2}} \cdot \cdots \cdot a^{(n-1)}_{x_{1,n-1}}\gamma - 1}{\pi^{i'_1}},$$

and

$$J = J_2[b_1],$$

for some unit parameters $x_{1,1}, x_{1,2}, \ldots, x_{1,n-1}$.

Our goal is to choose the unit parameters of b_1 so that

$$\langle J, H\rangle \subset R.$$

This duality relation is equivalent to

$$\langle w b_1^q, z_1^{\mu_1} z_2^{\mu_2} \cdot \cdots \cdot z_n^{\mu_n}\rangle \in R$$

for all $\mu_1, \ldots, \mu_2 \le p-1$ and for all q with $0 \le q \le p-1$ and all $w \in J_2$. But because H is a Hopf order, for $h \in H$,

$$\langle w b_1^q, h\rangle = \sum_{(h)} \langle b_1, h_{(1)}\rangle \langle b_1, h_{(2)}\rangle \cdot \ldots \cdot \cdot \langle b_1, h_{(q)}\rangle \langle w, h_{(q+1)}\rangle,$$

where $\Delta^q(h) = \sum_{(h)} h_{(1)} \otimes \cdots \otimes h_{(q+1)}$ (iterated Sweedler notation.) Since $\langle w, h_{(q+1)}\rangle$ is in R because $J_2 \subseteq H^*$, and $h_{(j)}$ is an R-linear combination of monomials in $z_1, \ldots, z_n$, it suffices to show that

$$\langle b_1, z_1^{\mu_1} z_2^{\mu_2} \cdot \cdots \cdot z_n^{\mu_n}\rangle \in R.$$

Thus, simplifying notation, we write

$$b_1 = b = \frac{a^{(1)}_{x_1} a^{(2)}_{x_2} \ldots a^{(n-1)}_{x_{n-1}}\gamma - 1}{\pi^{i'_1}},$$

where $x_k = x_{1,k}$, $1 \le k \le n-1$. We want to show that

$$\langle b, z_1^{\mu_1} z_2^{\mu_2} \cdot \cdots \cdot z_n^{\mu_n} \rangle \in R$$

for all $\mu_r, 0 \le \mu_r \le p-1$.

Since $\langle 1, z_1^{\mu_1} z_2^{\mu_2} \cdot \cdots \cdot z_n^{\mu_n} \rangle = 0$ unless all $\mu_r = 0$, and since $\langle b, 1 \rangle = 0$, it suffices to show that

$$\langle a_{x_1}^{(1)} a_{x_2}^{(2)} \dots a_{x_{n-1}}^{(n-1)} \gamma, z_1^{\mu_1} z_2^{\mu_2} \cdot \cdots \cdot z_n^{\mu_n} \rangle \in \pi^{i'_1} R \tag{1}$$

for all $\mu_r, 0 \le \mu_r \le p-1$, with $\mu_1 + \cdots + \mu_n > 0$.

To satisfy condition (1), we define $x_1, \dots, x_{n-1}$ so that for all $r > 1$,

$$\langle a_{x_1}^{(1)} a_{x_2}^{(2)} \dots a_{x_{n-1}}^{(n-1)} \gamma, z_r \rangle = 0. \tag{2}$$

Expanding the left side, we obtain

$$\begin{aligned} a_{x_1}^{(1)} & a_{x_2}^{(2)} \dots a_{x_{n-1}}^{(n-1)} \gamma \\ &= \sum_{r_0, \dots, r_{n-1}=0}^{p-1} x_1^{r_0} \cdot \cdots \cdot x_{n-1}^{r_{n-2}} \gamma e_{r_0 + pr_1 + \cdots + p^{n-1} r_{n-1}} \\ &= \sum_{r_0, \dots, r_{n-1}=0}^{p-1} (x_1 \zeta_n)^{r_0} \cdot \cdots \cdot (x_{n-1} \zeta_2)^{r_{n-2}} \zeta_1^{r_{n-1}} e_{r_0 + pr_1 + \cdots + p^{n-1} r_{n-1}}, \end{aligned}$$

and so, setting $x_n = 1$ and $\xi_{n-s} = x_{s+1} \zeta_{n-s}$ for $s = 0, \dots, n-1$, we have

$$\langle a_{x_1}^{(1)} a_{x_2}^{(2)} \dots a_{x_{n-1}}^{(n-1)} \gamma, g^{p^s} \rangle = x_{s+1} \zeta_{n-s} = \xi_{n-s}$$

for $s = 0, \dots, n-1$. Then

$$\langle a_{x_1}^{(1)} a_{x_2}^{(2)} \dots a_{x_{n-1}}^{(n-1)} \gamma, g^{p^{n-1} c_1} g^{p^{n-2} c_2} \dots g^{p c_{n-1}} g^{c_n} \rangle = \xi_1^{c_1} \xi_2^{c_2} \dots \xi_n^{c_n}$$

for $0 \le c_2, \dots, c_n \le p-1$ and any $c_1 \ge 0$, since for $c_1 = pq_1 + h_1$, with $0 \le h_1 < p$, $g^{p^{n-1} c_1} = g^{p^{n-1} h_1}$ and $\xi_1^{c_1} = \zeta_1^{c_1} = \zeta_1^{h_1} = \xi_1^{h_1}$. Thus any polynomial $f(X_1, \dots, X_n)$ in n variables of degree $\le p-1$ in each variable X_k with $k > 1$ has the property that

$$\langle a_{x_1}^{(1)} a_{x_2}^{(2)} \dots a_{x_{n-1}}^{(n-1)} \gamma, f(g^{p^{n-1}}, \dots, g^p, g) \rangle = f(\xi_1, \xi_2, \dots, \xi_n).$$

In particular, we have

$$\langle a_{x_1}^{(1)} a_{x_2}^{(2)} \dots a_{x_{n-1}}^{(n-1)} \gamma, z_r \rangle = u_{r,1}(\xi_1 - 1) + u_{r,2}(\xi_2 - 1) + \cdots + u_{r,r}(\xi_r - 1),$$

and so (2) is equivalent to

$$u_{r,1}(\xi_1 - 1) + u_{r,2}(\xi_2 - 1) + \cdots + u_{r,r}(\xi_r - 1) = 0.$$

Writing this last equation in matrix form allows us to determine $x_1, \dots, x_{n-1}$ precisely, as follows:

$$U \begin{pmatrix} \xi_1 - 1 \\ \xi_2 - 1 \\ \vdots \\ \xi_n - 1 \end{pmatrix} = \begin{pmatrix} u_{1,1}(\zeta_1 - 1) \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

which is equivalent to

$$\begin{pmatrix} \xi_1 - 1 \\ \xi_2 - 1 \\ \vdots \\ \xi_n - 1 \end{pmatrix} = \Theta \begin{pmatrix} u_{1,1}(\zeta_1 - 1) \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

since $\Theta U = I$. Thus we define the x_k, $1 \le k \le n-1$, so that

$$\zeta_r x_{n+1-r} - 1 = \xi_r - 1 = u_{1,1}(\zeta_1 - 1)\theta_{r,1},$$

for $r = 1, \dots, n$. Note that ξ_r is in R for all r since $e' > i_1$ and Θ has entries in R.

Now with $x_1, \dots, x_n$ defined as above, we proceed to show that the duality relation (1) is satisfied. For $r \ge 2$,

$$u_{r,1}(\xi_1 - 1) + u_{r,2}(\xi_2 - 1) + \cdots + u_{r,r}(\xi_r - 1) = 0,$$

and we may subtract the left side of this last equation from z_r to obtain for $r \ge 2$,

$$z_r = u_{r,1}(g^{p^{n-1}} - \xi_1) + u_{r,2}(g^{p^{n-2}} - \xi_2) + \cdots + u_{r,r}(g^{p^{n-r}} - \xi_r).$$

We set $y_s = g^{p^{n-s}} - \xi_s$ for $s = 1, \dots, n$. Then for $r > 1$,

$$z_r = \sum_{j=1}^{r} u_{r,j} y_j,$$

and

$$\begin{aligned} z_1 &= u_{1,1}(g^{p^{n-1}} - 1) \\ &= u_{1,1}(g^{p^{n-1}} - \zeta_1 + \zeta_1 - 1) \\ &= u_{1,1}(y_1 + \lambda), \end{aligned}$$

where $\lambda = \zeta_1 - 1$ has valuation e'.

The duality map

$$\Phi = \langle a^{(1)}_{x_1} a^{(2)}_{x_2} \dots a^{(n-1)}_{x_{n-1}} \gamma, - \rangle : KG \to K$$

then is a K-module homomorphism that maps $g^{p^{n-j}}$ to ξ_j for all j, hence maps y_r^q to 0 for $1 \le q \le p-1$, and so maps any polynomial $f(y_1, \dots, y_n)$ of degree $\leq p-1$ in $y_2, \ldots, y_n$ to $f(0, \ldots, 0)$. We need to show that

$$\Phi(z_1^{\mu_1} \ldots z_n^{\mu_n}) \in \pi^{i_1'} R$$

for all $\mu_1, \ldots, \mu_n$ not all 0.

Now

$$\begin{aligned} &z_1^{\mu_1} \ldots z_n^{\mu_n} \\ &\quad = (u_{1,1}y_1 + c)^{\mu_1}(u_{2,1}y_1 + u_{2,2}y_2)^{\mu_2} \cdot \cdots \cdot (u_{n,1}y_1 + \cdots + u_{n,n}y_n)^{\mu_n}, \end{aligned}$$

where $c = u_{1,1}\lambda$ is in R and $\mu_k \leq p-1$ for $1 \leq k \leq n$. This product is an R-linear combination of terms of the form

$$(u_{1,1}y_1)^{\nu_{1,1}}((u_{2,1}y_1)^{\nu_{2,1}}(u_{2,2}y_2)^{\nu_{2,2}}) \ldots ((u_{n,1}y_1)^{\nu_{n,1}} \ldots (u_{n,n}y_n)^{\nu_{n,n}}).$$

If we set

$$\overline{\nu}_s = (\nu_{s,s}, \nu_{s+1,s}, \ldots, \nu_{n,s})$$

and

$$|\overline{\nu}_s| = \nu_{s,s} + \nu_{s+1,s} + \cdots + \nu_{n,s}$$

and write

$$U_{-,s}^{\overline{\nu}_s} = u_{s,s}^{\nu_{s,s}} u_{s+1,s}^{\nu_{s+1,s}} \cdot \cdots \cdot u_{n,s}^{\nu_{n,s}}$$

for $s = 1, \ldots, n$, then $z_1^{\mu_1} \ldots z_n^{\mu_n}$ is an R-linear combination of terms of the form

$$B = U_{-,1}^{\overline{\nu}_1} U_{-,2}^{\overline{\nu}_2} \cdot \cdots \cdot U_{-,n}^{\overline{\nu}_n} y_1^{|\overline{\nu}_1|} y_2^{|\overline{\nu}_2|} \cdot \cdots \cdot y_n^{|\overline{\nu}_n|},$$

with $|\overline{\nu}_n| \leq p-1$. Write

$$\overline{U}_s = U_{-,s}^{\overline{\nu}_s} U_{-,s+1}^{\overline{\nu}_{s+1}} \cdot \cdots \cdot U_{-,n}^{\overline{\nu}_n}.$$

Note that for each r, the exponents $\nu_{r,1}, \nu_{r,2}, \ldots, \nu_{r,r}$ arise from expanding $z_r^{\mu_r}$, and hence

$$\nu_{r,1} + \nu_{r,2} + \cdots + \nu_{r,r} = \mu_r \leq p-1.$$

We wish to find conditions so that Φ maps each term B to $\pi^{i_1'} R$.

First observe that if the exponent $|\overline{\nu}_1|$ of y_1 is positive, then $\Phi(B) = 0$, since $\Phi(y_1^q f(y_2, \ldots, y_n)) = 0$ for any positive exponent q and any polynomial f. Thus we may assume $\overline{\nu}_1 = \overline{0}$.

Assume that $\overline{\nu}_1 = \cdots = \overline{\nu}_{s-1} = \overline{0}$, and $\overline{\nu}_s \neq \overline{0}$. Then

$$B = \overline{U}_s y_s^{|\overline{\nu}_s|} \ldots y_n^{|\overline{\nu}_n|}.$$

As given, B is not necessarily a polynomial of degree $\leq p-1$ in $y_2, \ldots, y_n$, but we will presently break B down into such polynomials. We need two lemmas.

Lemma 2.3. *For $s \leq t \leq n$, $y_t^p \equiv y_{t-1} + \beta_{t-1} \mod pRG$, with $\beta_{t-1} \in R$.*

Proof. We have $y_t = g^{p^{n-t}} - \xi_t$, so

$$\begin{aligned} y_t^p &\equiv g^{p^{n-t+1}} - \xi_t^p \\ &= g^{p^{n-t+1}} - \xi_{t-1} + \xi_{t-1} - \xi_t^p \\ &= y_{t-1} + \beta_{t-1} \end{aligned}$$

modulo pRG, where, since all ξ_r are in R,

$$\beta_{t-1} = \xi_{t-1} - \xi_t^p \in R. \qquad \square$$

LEMMA 2.4. *For* $t = 2, \dots, n$, $\operatorname{ord}(\beta_{t-1}) = i'_1 + \operatorname{ord}(\theta_{t-1,1})$. *Hence* $\operatorname{ord}(p) \geq \operatorname{ord}(\beta_{t-1}) > \operatorname{ord}(\beta_t)$ *for* $t = 2, \dots, n-1$.

Proof. We have

$$\begin{aligned} \beta_{t-1} &= \xi_{t-1} - \xi_t^p \\ &= 1 + u_{1,1}(\zeta_1 - 1)\theta_{t-1,1} - (1 + u_{1,1}(\zeta_1 - 1)\theta_{t,1})^p \\ &= u_{1,1}(\zeta_1 - 1)\theta_{t-1,1} - u_{1,1}^p(\zeta_1 - 1)^p\theta_{t,1}^p + pu_{1,1}(\zeta_1 - 1)x \end{aligned}$$

with $x \in R$. Since $\operatorname{ord}(u_{1,1}(\zeta_1 - 1)) = i'_1$, the second term above has valuation $\geq pi'_1 + pi'_t/2$. But $i_1 \leq (\frac{p-1}{p})e'$ by Theorem 2.1, hence $i'_1 \geq e'/p$, so $pi'_1 + pi_t/2 > e' = i'_1 + i_1 \geq i'_1 + \operatorname{ord}(\theta_{t-1,1})$. Moreover, the third term above has valuation $\geq e + i'_1$, and $e + i'_1 > i'_1 + \operatorname{ord}(\theta_{t-1,1})$. Thus the valuation of β_{t-1} is $i'_1 + \operatorname{ord}(\theta_{t-1,1})$.

Now

$$\operatorname{ord}(p) = e \geq e' = i_1 + i'_1 = i'_1 + \operatorname{ord}(\theta_{1,1}) = \operatorname{ord}(\beta_1),$$

and for all t we have

$$\operatorname{ord}(\theta_{t-1,1}) \geq \frac{1}{2}\operatorname{ord}(\theta_{t-1,t-1}) > \frac{p}{2}\operatorname{ord}(\theta_{t,t}) \geq \frac{p}{2}\operatorname{ord}(\theta_{t,1}),$$

hence $\operatorname{ord}(p) \geq \operatorname{ord}(\beta_{t-1}) > \operatorname{ord}(\beta_t)$ for $t = 2, \dots, n-1$. $\square$

Now assuming that B is not a polynomial of degree $\leq p-1$ in $y_2, \dots, y_n$, let t be the largest integer for which $|\overline{\nu}_t| \geq p$ (necessarily, $t < n$). Then B is of the form

$$\overline{U}_s y_s^{|\overline{\nu}_s|} \dots y_t^{|\overline{\nu}_t|} y_{t+1}^{r_{t+1}} \dots y_n^{r_n}$$

with $0 \leq r_{t+1}, \dots, r_n < p$. Write

$$|\overline{\nu}_t| = a_t p + r_t$$

with $0 \leq r_t < p$, and so

$$y_t^{|\overline{\nu}_t|} = (y_t^p)^{a_t} y_t^{r_t}$$

with

$$
\begin{aligned}
(y_t^p)^{a_t} &\equiv (y_{t-1} + \beta_{t-1})^{a_t} \mod pRG \\
&\equiv \sum_{k_t=0}^{a_t} \binom{a_t}{k_t} y_{t-1}^{k_t} \beta_{t-1}^{a_t-k_t},
\end{aligned}
$$

by Lemma 2.3. Substituting in B we find that modulo $\overline{U}_s pRG$, B is an R-linear combination of terms

$$B_{t-1} = \overline{U}_s y_s^{|\overline{\nu}_s|} \dots y_{t-1}^{|\overline{\nu}_{t-1}|+k_t} y_t^{r_t} \dots y_n^{r_n},$$

with $0 \le r_t, r_{t+1}, \dots, r_n \le p-1$ and $|\overline{\nu}_s| > 0$.

Next write

$$|\overline{\nu}_{t-1}| + k_t = a_{t-1}p + r_{t-1}$$

with $0 \le r_{t-1} < p$. Then

$$y_{t-1}^{|\overline{\nu}_{t-1}|+k_t} = (y_{t-1}^p)^{a_{t-1}} y_{t-1}^{r_{t-1}}$$

with

$$
\begin{aligned}
(y_{t-1}^p)^{a_{t-1}} &\equiv (y_{t-2} + \beta_{t-2})^{a_{t-1}} \mod pRG \\
&\equiv \sum_{k_{t-1}=0}^{a_{t-1}} \binom{a_{t-1}}{k_{t-1}} y_{t-2}^{k_{t-1}} \beta_{t-2}^{a_{t-1}-k_{t-1}},
\end{aligned}
$$

by Lemma 2.3. Substituting in the terms B_{t-1} we find that modulo $\overline{U}_s pRG$, B is an R-linear combination of terms

$$B_{t-2} = \overline{U}_s y_s^{|\overline{\nu}_s|} \dots y_{t-2}^{|\overline{\nu}_{t-2}|+k_{t-1}} y_{t-1}^{r_{t-1}} y_t^{r_t} \dots y_n^{r_n},$$

with $0 \le r_{t-1}, r_t, r_{t+1}, \dots, r_n \le p-1$ and $|\overline{\nu}_s| > 0$.

Repeating, we conclude that modulo $\overline{U}_s pRG$, B is an R-linear combination of terms of the form

$$B_s = \overline{U}_s y_s^{|\overline{\nu}_s|+k_{s+1}} y_{s+1}^{r_{s+1}} \dots y_n^{r_n},$$

with $0 \le r_{s+1}, r_{s+2}, \dots, r_n < p$, and $|\overline{\nu}_s| + k_{s+1} > 0$.

Write

$$|\overline{\nu}_s| + k_{s+1} = d_1 p^{s-1} + r_2 p^{s-2} + \dots + r_{s-1}p + r_s$$

with $0 \le r_i < p$ for $i = 2, \dots, s$, and $d_1 \ge 0$. Then

$$y_s^{|\overline{\nu}_s|+k_{s+1}} = y_s^{r_s} y_s^{pr_{s-1}} \dots y_s^{p^{s-2}r_2} y_s^{p^{s-1}d_1}.$$

Now by Lemma 2.3,

$$y_s^{p^r} \equiv (y_{s-1} - \beta_{s-1})^{p^{r-1}} \mod pRG,$$

and

$$(y_{s-1} - \beta_{s-1})^{p^{r-1}} \equiv y_{s-1}^{p^{r-1}} \mod \beta_{s-1}R.$$

Since by Lemma 2.4, $\mathrm{ord}(p) \geq \mathrm{ord}(\beta_1) > \cdots > \mathrm{ord}(\beta_{s-1})$, we have

$$y_s^{p^r} \equiv y_{s-1}^{p^{r-1}} \mod \beta_{s-1}RG.$$

Repeating, we obtain

$$y_s^{p^r} \equiv y_{s-r} \mod \beta_{s-1}RG$$

for all r, and so

$$y_s^{|\nu_s|+k_{s+1}} \equiv y_s^{r_s} y_{s-1}^{r_{s-1}} \dots y_2^{r_2} y_1^{d_1} \mod \beta_{s-1}RG.$$

Hence, modulo $\overline{U}_s\beta_{s-1}RG$, B is an R-linear combination of terms of the form

$$B_0 = \overline{U}_s y_1^{d_1} y_2^{r_2} \dots y_s^{r_s} \dots y_n^{r_n}$$

with $d_1 + r_2 + \cdots + r_s > 0$ and $r_2, \dots, r_n < p$. Hence $\Phi(B_0) = 0$.

Note that $\Phi(\overline{U}_s\beta_{s-1}RG) \subset \overline{U}_s\beta_{s-1}R$. Thus for the duality map Φ to send $z_1^{\mu_1} \dots z_n^{\mu_n}$ to $\pi^{i_1'}R$ for $\mu_1 + \cdots + \mu_n > 0$, it suffices that for each $s \geq 2$ we have

$$\beta_{s-1}\overline{U}_s \in \pi^{i_1'}R,$$

assuming that $|\overline{\nu}_1| = \cdots = |\overline{\nu}_{s-1}| = 0$.

Note

$$U_{-,s}^{\overline{\nu}_s} = \prod_{r=s}^{n} u_{r,s}^{\nu_{r,s}},$$

so we need that

$$\beta_{s-1}\overline{U}_s = \beta_{s-1}\prod_{t=s}^{n}\prod_{r=t}^{n} u_{r,t}^{\nu_{r,t}} = \beta_{s-1}\prod_{r=s}^{n}\prod_{t=s}^{r} u_{r,t}^{\nu_{r,t}} \in \pi^{i_1'}R, \tag{3}$$

where for $r = s, \dots, n$,

$$\sum_{t=s}^{n} \nu_{r,t} \leq p - 1.$$

In Lemma 2.4 we determined the valuation of β_{s-1} to be $i_1' + \mathrm{ord}(\theta_{s-1,1})$. We next determine the valuation of

$$\overline{U}_s = \prod_{r=s}^{n}\prod_{t=s}^{r} u_{r,t}^{\nu_{r,t}}.$$

LEMMA 2.5. *For $t \geq s$,*

$$\mathrm{ord}(u_{t,s}) \geq -\left(i_s + \frac{i_{s+1}}{2} + \frac{i_{s+2}}{2} + \cdots + \frac{i_t}{2}\right)$$

Proof. We have $\theta_{t,s} \geq i_t/2$ for $t > s$. We show

$$\mathrm{ord}(u_{s+k,s}) \geq -\left(i_s + \frac{i_{s+1}}{2} + \cdots + \frac{i_{s+k}}{2}\right)$$

by induction. The inequality is true for the trivial case $k = 0 : \mathrm{ord}(u_{s,s}) = i_s$. Assume the inequality holds for all s, t with $t - s < k$ and $k \geq 1$.

Since

$$u_{s+k,s}\theta_{s,s} + u_{s+k,s+1}\theta_{s+1,s} + \cdots + u_{s+k,s+k}\theta_{s+k,s} = 0$$

for $k \geq 1$,

$$\mathrm{ord}(u_{s+k,s}) + i_s \geq \min\{\mathrm{ord}(u_{s+k,s+r}) + \mathrm{ord}(\theta_{s+r,s})\},$$

where the minimum is taken over all $r = 1, \ldots, k$. Now

$$\begin{aligned} \mathrm{ord}(u_{s+k,s+r}) + \mathrm{ord}(\theta_{s+r,s}) &\geq i_{s+r}/2 - (i_{s+r} + i_{s+r+1}/2 + \cdots + i_{s+k}/2) \\ &= -(i_{s+r}/2 + i_{s+r+1}/2 + \cdots + i_{s+k}/2) \end{aligned}$$

by induction, for all $r = 1, \ldots, k$. So the minimum of

$$\mathrm{ord}(u_{s+k,s+r}) + \mathrm{ord}(\theta_{s+r,s})$$

for $r = 1, \ldots, k$ occurs when $r = 1$, since $i_{s+1} > i_{s+2} > \cdots > i_{s+k}$. Thus

$$\mathrm{ord}(u_{s+k,s}) + i_s \geq -(i_{s+1}/2 + i_{s+2}/2 + \cdots + i_{s+k}/2),$$

completing the proof. $\square$

For $s < t \leq r$ the lower bound on $\mathrm{ord}(u_{r,t})$ given by Lemma 2.5 is greater than or equal to the lower bound on $\mathrm{ord}(u_{r,t-1})$. Thus, since $\sum_{t=s}^{n} \nu_{r,t} \leq p-1$ for each $r \geq s$, we have

$$\mathrm{ord}(u_{r,s}^{\nu_{r,s}} u_{r,s+1}^{\nu_{r,s+1}} \cdot \cdots \cdot u_{r,r}^{\nu_{r,r}}) \geq -(p-1)\left(i_s + \frac{i_{s+1}}{2} + \frac{i_{s+2}}{2} + \cdots + \frac{i_r}{2}\right),$$

and so

$$\begin{aligned} \mathrm{ord}(\overline{U}_s) &\geq \sum_{r=s}^{n} -(p-1)\left(i_s + \frac{i_{s+1}}{2} + \frac{i_{s+2}}{2} + \cdots + \frac{i_r}{2}\right) \\ &= -(p-1)\left((n+1-s)i_s + (n-s)\frac{i_{s+1}}{2} + \cdots + \frac{i_n}{2}\right). \end{aligned}$$

Thus for (3) to hold, it suffices that

$$\mathrm{ord}(\beta_{s-1}) \geq i_1' + (p-1)\left((n+1-s)i_s + (n-s)\frac{i_{s+1}}{2} + \cdots + \frac{i_n}{2}\right)$$

for all $s \geq 2$. Since $\mathrm{ord}(\beta_{s-1}) = i_1' + \mathrm{ord}(\theta_{s-1,1})$ and $\mathrm{ord}(\theta_{s-1,1}) \geq i_{s-1}/2$, this follows from

$$\frac{i_{s-1}}{2} \geq (p-1)\left((n+1-s)i_s + (n-s)\frac{i_{s+1}}{2} + \cdots + \frac{i_n}{2}\right).$$

Now Theorem 2.1 requires the p-adic condition $i_{r-1} \geq di_r$ with $d \geq p$. Given the p-adic hypothesis $i_{s-1} \geq 2npi_s$ for all $s > 1$, this last inequality follows from

$$npi_s \geq (p-1)\left(ni_s + \frac{1}{2}\left(\frac{n-s}{2np} + \frac{n-s-1}{(2np)^2} + \cdots + \frac{1}{(2np)^{n-s}}\right) i_s\right),$$

which holds.

This completes the argument that $\langle J, H \rangle \subset R$, and so $J \subset H_\Theta^*$.

Now we need to show that $J = H_\Theta^*$. By induction, we know that $H_\Theta^* \cap K\hat{C}_{p^{n-1}} = J_2 = H_{\Theta_2}^*$. We have $J = J_2[\alpha]$ with $\alpha = (u\gamma - 1)/\pi^{i_1'}$, where

$$u = a_{x_1}^{(1)} a_{x_2}^{(2)} \ldots a_{x_{n-1}}^{(n-1)}.$$

Then

$$\alpha^p + \frac{1}{\pi^{pi_1'}} \sum_{r=1}^{p-1} \binom{p}{r} (\pi^{i_1'}\alpha)^r = \frac{u^p\gamma^p - 1}{\pi^{pi_1'}} \in H^* \cap K\hat{C}_{p^{n-1}} = J_2.$$

So J is free over J_2 with basis $1, \alpha, \ldots, \alpha^{p-1}$.

To show that $\operatorname{disc}(J) = \operatorname{disc}(H_\Theta^*)$, it suffices to show that

$$\operatorname{disc}(J) = \operatorname{disc}(J_2)^p \operatorname{disc}(H(i_1'))^{p^{n-1}}.$$

Now

$$\operatorname{disc}(J) = \operatorname{disc}(\{\beta_\nu \alpha^j\}),$$

where $\{\beta_\nu\}$ is an R-basis of J_2. Consider the basis

$$\{\beta_\nu \cdot (\pi^{i_1'}\alpha)^j\}$$

of $J_2[\pi^{i_1'}\alpha] = J_2[u\gamma]$. Then

$$\operatorname{disc}(\{\beta_\nu \cdot (\pi^{i_1'}\alpha)^j\}) = (\pi^{i_1' + 2i_1' + \cdots + (p-1)i_1'})^{2p^{n-1}} \operatorname{disc}(\{\beta_\nu \alpha^j\}).$$

Since $u = a_{x_1}^{(1)} \cdots a_{x_{n-1}}^{(n-1)}$ is in J_2 and $u\gamma = 1 + \pi^{i_1'}\alpha$ is a unit of J, hence of H_Θ, u is a unit of J_2, and so

$$J_2[u\gamma] = J_2[\gamma].$$

But this is clearly a Hopf order, and so

$$\begin{aligned}
\operatorname{disc}(J_2[\gamma]) &= \operatorname{disc}(J_2)^p \operatorname{disc}(RC_p)^{p^{n-1}} \\
&= \operatorname{disc}(\{\beta_\nu (\pi^{i_1'}\alpha)^j\}) \\
&= \pi^{2p^{n-1} i_1' p(p-1)/2} \operatorname{disc}(J).
\end{aligned}$$

But then

$$\begin{aligned}\operatorname{disc}(J) &= \operatorname{disc}(J_2)^p \left(\frac{\operatorname{disc}(RC_p)}{\pi^{i'_1 p(p-1)}}\right)^{p^{n-1}} \\ &= \operatorname{disc}(J_2)^p \left(\frac{p^p}{\pi^{i'_1 p(p-1)}}\right)^{p^{n-1}}\end{aligned}$$

and since $\operatorname{disc}(H(i'_1)) = (p/\pi^{i'_1(p-1)})^p$ by [Ch00, (22.16)], we conclude that

$$\operatorname{disc}(J) = \operatorname{disc}(J_2)^p \operatorname{disc}(H(i'_1))^{p^{n-1}} = \operatorname{disc}(H^*_\Theta).$$

Since $J \subset H^*_\Theta$, it follows that $J = H^*_\Theta$. This completes the proof. □

References

[By93] N. P. Byott, *Cleft extensions of Hopf algebras*, J. Algebra **157** (1993), 405–429. MR 94m:16043

[By02] ———, *Integral Hopf-Galois structures on degree p^2 extensions of p-adic fields*, J. Algebra **248** (2002), 334–365. MR 2002j:11142

[Ch95] L. N. Childs, *Hopf Galois structures on degree p^2 cyclic extensions of local fields*, New York J. Math. **2** (1996), 86–102 (electronic). MR 97j:11058

[Ch00] ———, *Taming wild extensions: Hopf algebras and local Galois module theory*, Mathematical Surveys and Monographs, vol. 80, American Mathematical Society, Providence, RI, 2000. MR 2001e:11116

[CS98] L. N. Childs and J. Sauerberg, *Degree two formal groups and Hopf algebras*, Mem. Amer. Math. Soc. **136** (1998), 55–89. MR 2000c:14067

[CU03] L. N. Childs and R. G. Underwood, *Cyclic Hopf orders defined by isogenies of formal groups*, Amer. J. Math. **125** (2003), 1295–1334. MR 2004i:11138

[Gr92] C. Greither, *Extensions of finite group schemes, and Hopf Galois theory over a complete discrete valuation ring*, Math. Z. **210** (1992), 37–67. MR 93f:14024

[GC98] C. Greither and L. N. Childs, *p-elementary group schemes-constructions, and Raynaud's theory*, Mem. Amer. Math. Soc. **136** (1998), 91–117. MR 2000c:14067

[La76] R. G. Larson, *Hopf algebra orders determined by group valuations*, J. Algebra **38** (1976), 414–452. MR 53 #8215

[Ra74] M. Raynaud, *Schémas en groupes de type $(p, \dots, p)$*, Bull. Soc. Math. France **102** (1974), 241–280. MR 54 #7488

[Sm97] H. Smith, *Constructing Hopf orders in elementary abelian group rings*, Doctoral dissertation, SUNY Albany, 1997.

[TO70] J. Tate and F. Oort, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. (4) **3** (1970), 1–21. MR 42 #278

[Un94] R. G. Underwood, *R-Hopf algebra orders in KC_{p^2}*, J. Algebra **169** (1994), 418–440. MR 95k:16055

[Un96] ———, *The valuative condition and R-Hopf algebra orders in KC_{p^3}*, Amer. J. Math. **118** (1996), 701–743. MR 97e:11150

[UC05] R. G. Underwood and L. N. Childs, *Duality for Hopf orders*, Trans. Amer. Math. Soc., to appear.

Lindsay N. Childs, Department of Mathematics and Statistics, University at Albany, Albany, NY 12222, USA
E-mail address: `childs@math.albany.edu`

Robert G. Underwood, Department of Mathematics, Auburn University Montgomery, Montgomery, AL 36124, USA
E-mail address: `runderwo@mail.aum.edu`