TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 358, Number 3, Pages 1117–1163
S 0002-9947(05)03728-1
Article electronically published on April 22, 2005

DUALITY FOR HOPF ORDERS

ROBERT G. UNDERWOOD AND LINDSAY N. CHILDS

Abstract. In this paper we use duality to construct new classes of Hopf orders in the group algebra KC_{p^3}, where K is a finite extension of $\mathbb{Q}_p$ and C_{p^3} denotes the cyclic group of order p^3. Included in this collection is a subcollection of Hopf orders which are realizable as Galois groups.

Introduction

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.

The classification of Hopf orders in KC_{p^n} is a problem that has been under investigation since the 1970's. Complete classifications are known only for the cases $n = 1, 2$; see [TO70], [La76], [Gr92], [By93], [Un94], [C00] and section 1, below. For $n = 3$ the first author constructed a class of Hopf orders by cohomological methods extending Greither's for $n = 2$ in [Gr92]. These Hopf orders are extensions of rank p Larson orders by rank p^2 Hopf orders that are duals of Larson orders, which we call *cohomological Hopf orders*. In [CU03] we constructed Hopf orders in KC_{p^n} for all n using isogenies of polynomial formal groups, orders that we will call *formal group Hopf orders*. We showed that for $n = 3$ there exist formal group Hopf orders that are not cohomological.

Classifying Hopf orders in KC_{p^n} remains open for $n \geq 3$.

This paper uses duality to construct new Hopf orders in KC_{p^3}.

The paper contains five sections.

In section 1, we review the structure of R-Hopf orders in KC_p and KC_{p^2}. Assuming K contains ζ_2, a primitive p^2nd root of unity, we give a new duality construction of all Hopf orders in KC_{p^2}. We then define "triangular" Hopf orders in KC_{p^3}, recall and re-parametrize as triangular Hopf orders the cohomological Hopf orders in KC_{p^3} from [Un96], and introduce ILD Hopf orders in KC_{p^3}, a collection of triangular Hopf orders induced from cohomological Hopf orders by base change from the dual Larson orders defining the cohomological Hopf orders.

Section 2 is devoted to duality results needed later in the paper. Included is a precise determination of the valuation of $G(x, y) - 1$, where $G(x, y)$ is the Gauss sum defined in [GC98]. As a consequence of these duality results, we show that

Received by the editors July 18, 2003 and, in revised form, April 16, 2004.
2000 *Mathematics Subject Classification.* Primary 13C05, 13E15, 16W30; Secondary 14L05, 12F10.

most triangular Hopf orders are induced Hopf orders, that is, are "induced from both ends" from a cohomological Hopf order (Theorem 2.8).

Section 3 contains the generalization to KC_{p^3} of the duality construction of Section 1. The triangular Hopf orders obtained are called *duality Hopf orders*. This collection is distinct from the collection of ILD orders.

In section 4, we recall the class of *formal group Hopf orders* ([CU03]). For $n = 3$ we find inequalities on the parameters sufficient for the existence of formal group Hopf orders, independent of and sharper than the main result of [CU03], and recall from [CU03] that under suitable conditions on the parameters, a formal group Hopf order is not a triangular Hopf order. We find that the dual of any formal group Hopf order is a triangular Hopf order that is never itself a formal group Hopf order. We find conditions for a formal group Hopf order itself to be triangular.

Finally, in section 5, we show that almost none of the Hopf orders of rank p^3 defined in this paper are realizable. By a theorem of N. Byott [By04], a Hopf order H with local dual H^* is realizable if and only if H^* is monogenic as an R-algebra. For known realizable Hopf orders of rank p^2 and p^3 we find algebra generators for their duals, and we find a new class of realizable Hopf orders of rank p^3. This new class includes triangular Hopf orders that are not among any of the families constructed in sections 1, 3 and 4. We conjecture that we have not constructed all realizable Hopf orders of rank p^3, and so the problem of constructing all Hopf orders of rank p^n, $n \geq 3$, remains open.

The first author thanks the University at Albany for its hospitality during this research; the second author thanks Auburn University Montgomery and Union College for their hospitality during this research. Both authors thank the referee for a thorough reading of this paper; the resulting comments and suggestions improved the content and presentation of this work.

1. Known Hopf orders of rank p, p^2, p^3

Assume K is a field containing $\mathbb{Q}_p$ and a primitive pth root of unity ζ_1. Let $\mathrm{ord}(\zeta_1 - 1) = e', \mathrm{ord}(p) = e = (p-1)e'$. For an integer i with $0 \leq i \leq e'$, set $i' = e' - i$.

Orders in KC_p. Orders in KC_p were classified by J. Tate and F. Oort [TO70], (cf. [C00, Chapters 4 and 5]). It is convenient to describe them as follows: any R-Hopf order in KC_p is of the form

$$H(i) = R\left[\frac{g-1}{\pi^i}\right],$$

$\langle g \rangle = C_p$, for some integer i, $0 \leq i \leq e'$. Such R-Hopf orders are called *Larson orders in KC_p* [La76], [Un94].

Assuming K contains a primitive pth root of unity ζ_1, the character group $\hat{C}_p$ of C_p is isomorphic to C_p, and is generated by the character γ with $\gamma^j(g^k) = \zeta_1^{jk}$ for $j, k = 0, \ldots, p-1$. The linear dual of $H(i)$ is then the Larson order

$$H(i') = R\left[\frac{\gamma-1}{\pi^{i'}}\right];$$

cf. [Gr92, Lemma 3.1] or [C00, 21.2].

Orders in KC_{p^2}. Hopf orders in KC_{p^2} were classified by Byott [By93], Greither [Gr92] and Underwood [Un94], assuming that K contains a primitive pth root of unity ζ_1. Let $C_{p^2} = \langle g \rangle$ and let

$$e_m = \frac{1}{p} \sum_{k=0}^{p-1} \zeta_1^{-mk} g^{pk}, 0 \leq m \leq p-1,$$

denote the minimal idempotents of $K\langle g^p \rangle$. Greither's classification of Hopf orders in KC_{p^2} uses elements of $K\langle g^p \rangle$ defined as follows: define

$$a : K^* \to K\langle g^p \rangle^*$$

by sending v in K^* to $a_v = \sum_{m=0}^{p-1} v^m e_m$. Then a is a multiplicative homomorphism, with $a_1 = 1$ and $a_{\zeta_1} = g^p$. Greither showed that for $v \in R$,

$$a_v - 1 \text{ is in } \pi^\ell H(i) \text{ iff } \operatorname{ord}(v-1) \geq i' + \ell. \tag{1}$$

Using a cohomological argument, Greither showed that given i, j with $0 \leq i, j \leq e'$ satisfying the "p-adic" condition $pj \leq i$, the order

$$H(i,j,v) = R\left[\frac{g^p - 1}{\pi^i}, \frac{a_v g - 1}{\pi^j}\right] = H(i)\left[\frac{a_v g - 1}{\pi^j}\right]$$

is a Hopf order in KC_{p^2} provided that

$$\operatorname{ord}(v-1) \geq max\{\lceil i' + j/p \rceil, \lceil i'/p + j \rceil\},$$

where $\lceil x \rceil$ denotes the smallest positive integer $\geq x$. The map sending g to $\overline{g}$ (= the coset of g modulo $\langle g^p \rangle$) induces a short exact sequence of Hopf algebras,

$$K \to K\langle g^p \rangle \to KC_{p^2} \to K\langle \overline{g} \rangle \to K$$

and a sequence of Hopf orders,

$$R \to H(i) \to H(i,j,v) \to H(j) \to R.$$

Thus Greither's orders are naturally presented as extensions of rank p Larson orders, and in fact that is how they were constructed.

If $v = 1$, or more generally, if $\operatorname{ord}(v-1) \geq i' + j$, then $H(i,j,v)$ is isomorphic to the Larson order $H(i,j,1) := H(i,j)$ (which is only defined if the p-adic condition $pj \leq i$ holds). Generally, we have from [Gr92] (cf. [C00, (31.12)]),

$$H(i,j,v) \equiv H(i,j,w) \text{ iff } \operatorname{ord}(v-w) \geq i' + j.$$

Suppose K contains a primitive p^2nd root of unity ζ_2 with $\zeta_1 = \zeta_2^p$. Let $\hat{C}_{p^2} = \langle \gamma \rangle$ be the character group of C_{p^2} and let

$$\hat{e}_m = \frac{1}{p} \sum_{k=0}^{p-1} \zeta_1^{-mk} \gamma^{pk}, 0 \leq m \leq p-1,$$

denote the minimal idempotents of $K\langle \gamma^p \rangle$. Then the linear dual of $H(i,j,v)$ is the Hopf order $H(j', i', \hat{v})$ in $K\langle \gamma \rangle$, where $\hat{v} = (v\zeta_2)^{-1}$, as will be verified below.

Underwood [Un94] showed that every Hopf order in KC_{p^2} is either a Greither order or the dual of a Greither order.

As a model for a construction in section 3, we now give a new construction of Hopf orders in KC_{p^2}. Our approach is based on the following result, [C00, (31.2)], which is a slight generalization of [GC98, Lemma 2.1].

Proposition 1.1. *Let G be a finite p-group, and let G' be a subgroup of index p, with $G = \langle G', g\rangle$. Let A be a Hopf order in KG'. Let u be a non-zero element of KG' and $0 \le k \le e'$. Then*

$$H = A[y],\ y = \frac{ug-1}{\pi^k},$$

is an order in KG, free over A with basis $\{1, y, \dots, y^{p-1}\}$, iff

$$g^p u^p \equiv 1 \pmod{\pi^{pk}A},$$

and is a Hopf order in KG if in addition, u is a unit of A and

$$\Delta(u) \equiv u \otimes u \pmod{\pi^k(A \otimes A)}.$$

In Proposition 1.1 the algebra condition $g^p u^p \equiv 1 \pmod{\pi^{pk}A}$ is generally easier to understand than the coalgebra condition $\Delta(u) \equiv u \otimes u \pmod{\pi^k(A \otimes A)}$.

In Section 31 of [C00], Hopf orders in KC_{p^2} were constructed using Proposition 1.1, applying both the algebra and coalgebra conditions. However, if we assume K contains ζ_2, we can construct the same Hopf orders using only the algebra condition and duality. Denote $(\zeta_2 v)^{-1} = \hat{v}$. Then $\mathrm{ord}(\zeta_2 v - 1) = \mathrm{ord}(\hat{v} - 1)$.

Theorem 1.2. *Assume K contains ζ_2, a primitive p^2nd root of unity, let $0 \le i, j \le e'$, and let v be a unit in R. Let*

$$A(i,j,v) = R\left[\frac{g^p - 1}{\pi^i}, \frac{a_v g - 1}{\pi^j}\right]$$

and assume that v satisfies the algebra condition

$$\mathrm{ord}(\zeta_1 v^p - 1) \ge i' + pj.$$

Let

$$A(j', i', \hat{v}) = R\left[\frac{\gamma^p - 1}{\pi^{j'}}, \frac{a_{\hat{v}}\gamma - 1}{\pi^{i'}}\right]$$

with $\langle\gamma\rangle = \hat{C}_{p^2}$, and assume that $\hat{v}$ satisfies the algebra condition

$$\mathrm{ord}(v^p - 1) \ge j + pi'.$$

Then $A(i,j,v)$ is an R-Hopf order in KC_{p^2}.

Proof. First observe that $(a_v g)^p = a_{v^p} a_{\zeta_1} = a_{v^p\zeta_1}$, and so by (1),

$$(a_v g)^p \equiv 1 \pmod{\pi^{pj}H(i)} \quad \text{iff} \quad v^p\zeta_1 \equiv 1 \pmod{\pi^{i'+pj}R}.$$

Thus Proposition 1.1 implies that $A(i,j,v)$ is an algebra that is free of rank p over $H(i)$. Similarly for $A(j', i', \hat{v})$. Now let $A(i,j,v)^*$ denote the linear dual of $A(i,j,v)$. Let $tr: KC_{p^2} \to K$ be the trace map defined by $tr(x) = \sum_{i=0}^{p^2-1} \sigma_i(x)$, where $\sigma_i: KC_{p^2} \to K$ is given by $\sigma_i(g) = \zeta_2^i$. Let $\{\alpha_j\}$ be an R-basis for $A(i,j,v)$. Then there exists a collection $\{\beta_j\} \subseteq KC_{p^2}$ for which $tr(\alpha_i\beta_j) = \delta_{ij}$, where δ_{ij} is Kronecker's symbol. One has that

$$A(i,j,v)^* = \{x \in KC_{p^2} | tr(xA(i,j,v)) \subseteq R\},$$

and $A(i,j,v)^*$ is a free R-module with basis $\{\beta_j\}$.

If we show that $A(j', i', \hat{v}) = A(i,j,v)^*$, then $A(i,j,v)^*$ will be closed under the multiplication map induced by the multiplication on $K\hat{C}_{p^2}$, which means that $A(i,j,v)$ will be closed under the comultiplication induced by that on KC_{p^2}, and hence $A(i,j,v)$ will be an R-order and an R-coalgebra. It will then follow that

$A(i,j,v)$ is closed under the antipode, and consequently, $A(i,j,v)$ will be an R-Hopf order in KC_{p^2}.

To show that $A(j',i',\hat{v}) = A(i,j,v)^*$ we first show that their discriminants are equal.

By the method of [Un94, Theorem 2.0, Part 2], one has

$$disc(A(i,j,v)) = \pi^{p^2(p-1)(i'+j')}R$$

and

$$disc(A(j',i',\hat{v})) = \pi^{p^2(p-1)(i+j)}R.$$

(Note: this shows that the discriminant of $A(i,j,v)$ depends only on i and j.)

Let M be the matrix which multiplies the basis

$$\left\{ \left(\frac{g^p-1}{\pi^i}\right)^a \left(\frac{a_v g-1}{\pi^j}\right)^b \right\}$$

of $A(i,j,v)$ to give a basis of RC_{p^2}. Then

$$disc(RC_{p^2}) = det^2(M)disc(A(i,j,v)).$$

Moreover, M^T is the matrix which multiplies a basis of the maximal integral order $(RC_{p^2})^* = R^{p^2}$ to give a basis for $A(i,j,v)^*$, hence

$$\begin{aligned} disc(A(i,j,v)^*) &= det^2(M^T)disc(R^{p^2}) \\ &= det^2(M)disc(R^{p^2}). \end{aligned}$$

Now by a well-known formula, $disc(RC_{p^2})disc(R^{p^2}) = \pi^{2p^2e}R$, thus

$$disc(A(i,j,v))disc(A(i,j,v)^*) = \pi^{2p^2e}R,$$

whence $disc(A(i,j,v)^*) = \mathrm{disc}(A(j',i',\hat{v}))$.

We next show that

$$\langle A(i,j,v), A(j',i',\hat{v})\rangle \subseteq R,$$

that is,

$$\langle (g^p-1)^q(a_v g-1)^r, (\gamma^p-1)^s(a_{\hat{v}}\gamma-1)^t\rangle \in \pi^{qi+rj+sj'+ti'}R$$

for $q,r,s,t = 0,\ldots,p-1$. Here $\langle\ ,\ \rangle :\ KC_{p^2}\times K\hat{C}_{p^2} \mapsto K$ is the duality map.

We need the following lemma, whose proof is a routine computation left to the reader.

Lemma 1.3. *Let e_i denote the minimal idempotents of KC_p. Then*

$$\langle e_j g^{pa+b}, e_k\gamma^{pc+d}\rangle = \zeta_2^{(pa+b)(pc+d)}$$

if $j=d$, $k=b$, and is 0 otherwise.

Let $S = \langle (g^p-1)^q(a_v g-1)^r, (\gamma^p-1)^s(a_{\hat{v}}\gamma-1)^t\rangle$, and let $\sum_{c,d,e,f=0}^{q,r,s,t}$ denote the sum $\sum_{c=0}^{q}\sum_{d=0}^{r}\sum_{e=0}^{s}\sum_{f=0}^{t}$. Then

$$\begin{aligned}
S &= \sum_{c,d,e,f=0}^{q,r,s,t} C(c,d,e,f)\langle g^{pc}(a_v g)^d, \gamma^{pe}(a_{\hat{v}}\gamma)^f\rangle \\
&= \sum_{c,d,e,f=0}^{q,r,s,t} C(c,d,e,f)\langle a_{v^d} g^{pc+d}, a_{\hat{v}^f}\gamma^{pe+f}\rangle \\
&= \sum_{c,d,e,f=0}^{q,r,s,t} C(c,d,e,f)\sum_{i,j} v^{di}\hat{v}^{fj}\langle e_i g^{pc+d}, e_j\gamma^{pe+f}\rangle \\
&= \sum_{c,d,e,f=0}^{q,r,s,t} C(c,d,e,f)v^{df}\hat{v}^{df}\zeta_2^{(pc+d)(pe+f)} \qquad \text{(by Lemma 1.3)} \\
&= \sum_{c,d,e,f=0}^{q,r,s,t} C(c,d,e,f)(v\hat{v}\zeta_2)^{df}\zeta_1^{cf+ed},
\end{aligned}$$

where

$$C(c,d,e,f) = \binom{q}{c}\binom{r}{d}\binom{s}{e}\binom{t}{f}(-1)^{q-c}(-1)^{r-d}(-1)^{s-e}(-1)^{t-f}.$$

Since $\hat{v}$ is so that $v\hat{v}\zeta_2 = 1$,

$$\begin{aligned}
S &= \sum_{c,d,e,f=0}^{q,r,s,t}\binom{q}{c}\binom{r}{d}\binom{s}{e}\binom{t}{f}(-1)^{q-c}(-1)^{r-d}(-1)^{s-e}(-1)^{t-f}\zeta_1^{cf+ed} \\
&= \left(\sum_{c,f=0}^{q,t}\binom{q}{c}\binom{t}{f}(-1)^{q-c}(-1)^{t-f}\zeta_1^{cf}\right)\left(\sum_{d,e=0}^{r,s}\binom{r}{d}\binom{s}{e}(-1)^{r-d}(-1)^{s-e}\zeta_1^{ed}\right).
\end{aligned}$$

Suppose $q \geq t$. Then considering the left sum,

$$\begin{aligned}
\sum_{c,f=0}^{q,t}\binom{q}{c}\binom{t}{f}(-1)^{q-c}(-1)^{t-f}\zeta_1^{cf} &= \sum_{f=0}^{t}\binom{t}{f}(-1)^{t-f}\left(\sum_{c=0}^{q}\binom{q}{c}(-1)^{q-c}(\zeta_1^f)^c\right) \\
&= \sum_{f=0}^{t}\binom{t}{f}(-1)^{t-f}(\zeta_1^f-1)^q,
\end{aligned}$$

and since $(\zeta_1-1)^q$ divides every term of the sum, the order of the left sum is at least

$$qe' = qi + qi' \geq qi + ti'.$$

Since the same argument will work if $t \geq q$, and will also work with the right sum (involving d and e), it follows that S has order $\geq qi + ti' + rj + sj'$, as we wished to show. Therefore $A(j',i',\hat{v}) = A(i,j,v)^*$, and so $A(i,j,v)$ is an R-Hopf order, completing the proof. □

Remark 1.4. Consider the units v and $\hat{v}$ of Theorem 1.2. Since $\mathrm{ord}(\zeta_2 - 1) = e'/p$, we have the following possibilities:

(1) If $\mathrm{ord}(\hat{v} - 1) > e'/p$, then $\mathrm{ord}(v - 1) = e'/p$.
(2) If $\mathrm{ord}(v - 1) > e'/p$, then $\mathrm{ord}(\hat{v} - 1) = e'/p$.
(3) If $\mathrm{ord}(v - 1) \leq e'/p$ and $\mathrm{ord}(\hat{v} - 1) \leq e'/p$, then $\mathrm{ord}(v - 1) = \mathrm{ord}(\hat{v} - 1)$.

The hypotheses of Theorem 1.2, namely, $\mathrm{ord}(v^p - 1) \geq pi' + j$ and $\mathrm{ord}(\zeta_1 v^p - 1) \geq i' + pj$, imply that $e' \geq i' + j/p$ and $e' \geq i'/p + j$. Thus by Lemma 3.3, $\mathrm{ord}(v - 1) \geq i' + j/p$ and $\mathrm{ord}(\hat{v} - 1) \geq i'/p + j$. We then have:

- In Case 1, $e'/p = \mathrm{ord}(v - 1) \geq i' + j/p$, hence $j'/p \geq i'$, the dual p-adic condition on i and j. Also, $\mathrm{ord}(\hat{v} - 1) \geq \mathrm{ord}(v - 1) \geq i' + j/p$ and $\mathrm{ord}(\hat{v} - 1) \geq i'/p + j$, so $A(j', i', \hat{v})$ is Greither.
- In Case 2, $e'/p = \mathrm{ord}(\hat{v} - 1) \geq i'/p + j$, hence $i \geq pj$, the p-adic condition on i and j. Also, $\mathrm{ord}(v-1) \geq \mathrm{ord}(\hat{v}-1) \geq i'/p+j$ and $\mathrm{ord}(v-1) \geq i'+j/p$, so $A(i, j, v)$ is Greither.
- In Case 3, $e'/p \geq \mathrm{ord}(v - 1) \geq i' + j/p$, hence $j'/p \geq i'$, and also $e'/p \geq \mathrm{ord}(\hat{v} - 1) \geq i'/p + j$, hence $i \geq pj$, and both the p-adic and dual p-adic conditions hold. Also, since $\mathrm{ord}(v - 1) = \mathrm{ord}(\hat{v} - 1)$, both $A(i, j, v)$ and $A(j', i', \hat{v})$ are Greither.

Thus in Theorem 1.2, i and j always satisfy either the p-adic or dual p-adic condition, and either $A(i, j, v)$ or $A(j', i', \hat{v})$ is a Greither order.

Theorem 1.5. *The construction of Theorem* 1.2 *yields every Hopf order in* KC_{p^2}

Proof. In [Un94] the first author proved that every Hopf order in KC_{p^2} is either a Greither order or the dual of a Greither order. Thus it suffices to show that every Greither order $H(i, j, v)$, that is, an order of the form $A(i, j, v)$, where $i \geq pj$ and v satisfies

$$\mathrm{ord}(v - 1) \geq i' + j/p \text{ and } \mathrm{ord}(v - 1) \geq i'/p + j,$$

is of the form $A(i, j, v)$ in Theorem 1.2. For that we only need to show that if $i \geq pj$ and v satisfies $\mathrm{ord}(v - 1) \geq i' + j/p$ and $\mathrm{ord}(v - 1) \geq i'/p + j$, then

$$\mathrm{ord}(\zeta_2 v - 1) \geq i'/p + j, \tag{2}$$

so that the valuation hypotheses on $\zeta_1 v^p - 1$ and $v^p - 1$ in Theorem 1.2 hold. If $\mathrm{ord}(\zeta_2 v - 1) \geq \mathrm{ord}(v - 1)$, as in cases (1) and (3) of Remark 1.4, then (2) is clear. Otherwise, we are in case (2) of Remark 1.4, so the p-adic condition on i and j gives $i/p \geq j$, so $e'/p \geq i'/p + j$, and hence

$$\mathrm{ord}(\zeta_2 v - 1) \geq i'/p + j.$$

□

Note also that in either case, $i \geq j$ (and, equivalently, $j' \geq i'$); cf. [Un94, Theorem 1.3.1].

We conclude this subsection on rank p^2 Hopf orders by looking at the relationship between general Hopf orders in KC_{p^2} and Larson orders.

Let $A(i, j, v)$ be an R-Hopf order in KC_{p^2}. Then $A(i, j, v)$ contains a largest Larson order, denoted by $\mathcal{L}(A(i, j, v))$. Necessarily, $\mathcal{L}(A(i, j, v)) = H(i, l)$, where $l = j$ if $\mathrm{ord}(1 - v) \geq i' + j$, and $l = i - e' + \mathrm{ord}(1 - v)$, that is, $\mathrm{ord}(1 - v) = i' + l$ otherwise ([Un94, Theorem 1.4.0]).

Under certain conditions $A(i,j,v)$ also contains a "largest Larson dual", that is, the maximal R-Hopf order in KC_{p^2} of the form $H(s,r)^*$ which is contained in $A(i,j,v)$. We denote this Hopf order by $\mathcal{LD}(A(i,j,v))$. Assuming K contains ζ_2, if $H(s,r)^*$ is contained in $A(i,j,v)$, then $A(i,j,v)^*$ is contained in $H(s,r)$; hence the largest Larson dual in $A(i,j,v)$ is the dual of the smallest Larson order containing $A(i,j,v)^* = A(j',i',\hat{v})$.

Lemma 1.6. *Let $A(i,j,v)$ be an R-Hopf order in KC_{p^2} and set $\hat{v} = v^{-1}\zeta_2^{-1}$.*
If $j' \geq pi'$ and $\operatorname{ord}(\hat{v}-1) \geq i'+j$, then $A(i,j,v) = H(j',i')^*$ is a Larson dual.
If $e'/p \geq i'$ and $\operatorname{ord}(\hat{v}-1) = i'+\varrho$ with $\varrho < j$, then $\mathcal{LD}(A(i,j,v)) = H(\varrho',i')^*$.

Proof. The first case follows from remarks near the beginning of this subsection. For the case when $A(i,j,v)$ is not a Larson dual, we seek ϱ' minimal $\geq j'$ so that $H(\varrho',i')$ is Larson, hence

$$pi' \leq \varrho' \leq e',$$

and $A(j',i',\hat{v}) \subset A(\varrho',i',\hat{v}) = H(\varrho',i')$, hence

$$\operatorname{ord}(1-\hat{v}) \geq i'+\varrho.$$

We let $\operatorname{ord}(1-\hat{v}) = i'+\varrho$ with $\varrho < j$, and show

$$pi' \leq \varrho' \leq e'.$$

If so, then $H(\varrho',i')$ is Larson and minimal containing $A(j',i',\hat{v})$, so $H(\varrho',i')^*$ is the largest Larson dual contained in $A(i,j,v)$.

We consider the cases of Remark 1.4: In cases (1) and (3), we have $j' \geq pi'$, and since $\varrho' > j'$, we have $\varrho' \geq pi'$. Also,

$$i'+\varrho = \operatorname{ord}(\hat{v}-1) \geq \operatorname{ord}(v-1) \geq i'+j/p,$$

hence $\varrho \geq 0$, hence $\varrho' \leq e'$.

In case (2), $\operatorname{ord}(\hat{v}-1) = i'+\varrho = e'/p \geq i'$ by hypothesis, so $\varrho \geq 0$; also,

$$\begin{aligned}\varrho' &= i'+e'-e'/p \\ &= i'+\left(\frac{p-1}{p}\right)e' \\ &\geq i'+\left(\frac{p-1}{p}\right)pi' = pi'.\end{aligned}$$

□

Orders in KC_{p^3}. We first review the class of R-Hopf orders in KC_{p^3} constructed in [Un96].

Let H be an arbitrary R-Hopf order in KC_{p^3}. Then H induces the short exact sequences of Hopf orders

$$R \to A(i,j,u) \to H \to H(k) \to R$$

and

$$R \to H(i) \to H \to A(j,k,w) \to R,$$

where $A(i,j,u)$ and $A(j,k,w)$ are Hopf orders in KC_{p^2}, and $H(i)$ and $H(k)$ are Larson orders in KC_p. It follows that H is of the form

$$H = R\left[\frac{g^{p^2}-1}{\pi^i}, \frac{a_u g^p - 1}{\pi^j}, \Upsilon\right],$$

where Υ is some element of H mapping to $\frac{a_w h-1}{\pi^k}$ in $A(j,k,w)$, where h is g (mod $\langle g^{p^2}\rangle$). If Υ is of the form

$$\frac{a_v b_w g-1}{\pi^k},$$

where

$$b_w = \sum_{0\le pa+b\le p^2-1} w^a e_{pa+b}$$

so that

$$H = A(i,j,u)\left[\frac{a_v b_w g-1}{\pi^k}\right] = R\left[\frac{g^{p^2}-1}{\pi^i}, \frac{a_u g^p-1}{\pi^j}, \frac{a_v b_w g-1}{\pi^k}\right],$$

then we call H a *triangular Hopf order*. Here

$$e_{pa+b} = \frac{1}{p^2}\sum_{r,s=0}^{p-1} \zeta_2^{-(pa+b)(pr+s)} g^{p(pr+s)}$$

for $0\le a,b\le p-1$ are the pairwise orthogonal minimal idempotents of $KC_{p^2}, C_{p^2} = \langle g^p\rangle$. In what follows we shall denote the R-algebra $R\left[\frac{g^{p^2}-1}{\pi^i}, \frac{a_u g^p-1}{\pi^j}, \frac{a_v b_w g-1}{\pi^k}\right]$ by $H(i,j,k,u,v,w)$.

Analogous to the elements a_u, the elements b_w are multiplicative:

$$b_y b_w = b_{yw}$$

(clear, since the e_{pa+b} are idempotents). One may verify that b_w maps to a_w under the map from H to $A(j,k,w)$.

In [CU03] a Hopf order H in KC_{p^3} was called a cohomological Hopf order if

$$H = A(i,j,u)\left[\frac{b_{v,w} g-1}{\pi^k}\right],$$

where

$$b_{v,w} = \sum_{0\le pa+b\le p^2-1} v^b w^{pa+b} e_{pa+b}.$$

Then $b_{w^p} = b_{w^{-1},w}$, and since

$$e_b^1 = \sum_{a=0}^{p-1} e_{pa+b}^2,$$

where e_b^1, $b=0,\dots,p-1$, are the minimal idempotents of KC_p, $C_p = \langle g^{p^2}\rangle$, and $e_{pa+b}^2 = e_{pa+b}$, it follows easily that $b_{v,1} = a_v$, and so

$$b_{v,w} = b_{vw,1} b_{w^{-1},w} = a_{vw} b_{w^p}.$$

Thus the cohomological Hopf orders of [CU03] are included in the class of triangular Hopf orders described above. Note that

$$g^p = b_{1,\zeta_2} = b_{\zeta_2,1} b_{\zeta_2^{-1},\zeta_2} = a_{\zeta_2} b_{\zeta_1}.$$

We now introduce a collection of triangular Hopf orders constructed in [Un96, §4.1, §4.2].

Let $U(R)$ denote the group of units in R. Let $pi' \le j'$, $H(j',i')$ be the Larson order in KC_{p^2}, and let $H(j',i')^* = A(i,j,\zeta_2^{-1})$ be its linear dual. Let $H(k)$ denote a Larson order in KC_p for which $pk\le l$, where $H(i,l) = \mathcal{L}(H(j',i')^*)$ is the largest

Larson order contained in $H(j',i')^*$. Then $l = j$ if $e'/p \geq i' + j$, and otherwise, $l = e'/p - i'$ (≥ 0 since $pi' \leq j' \leq e'$). (Note that $pl = e' - pi' < e' - i' = i$, so i and l are p-adic.) Let

$$\mathrm{Ext}^1(\mathrm{Spec}\ H(j',i')^*, \mathrm{Spec}\ H(k))$$

denote the collection of 1-extensions of Spec $H(k)$ by Spec $H(j',i')^*$.

Here is the main result of [Un96] (cf. [CU03, Theorem 4.0]):

Theorem 1.7. *Assume $pi' \leq j', pk \leq j$ and $i' + pk \leq e'/p$. Let M be the group of pairs $(v,w) \in U(R) \times U(R)$ such that*

(A) $\mathrm{ord}(v-1) \geq i'/p + k$,
(B) $\mathrm{ord}(w-1) \geq j'/p + k$,
(C) $\mathrm{ord}(w-1) \geq j' + k/p$,
(D) $\mathrm{ord}(v^p w^{-1} - 1) \geq pi' + k$,

and let N be the subgroup of M consisting of pairs (v,w) such that $\mathrm{ord}(v-1) \geq i'+k$ *and* $\mathrm{ord}(w-1) \geq j'+k$. *Then the classes $[(v,w)]$ in M/N are in* 1-1 *correspondence with elements in $Ext^1(Spec\ H(j',i')^*, Spec\ H(k))$, $pk \leq l$, which over K appear as $\mu_{p,K} \longrightarrow \mu_{p^3,K} \longrightarrow \mu_{p^2,K}$. The class $[(v,w)]$ corresponds to a short exact sequence of R-Hopf orders*

$$R \to H(j',i')^* \longrightarrow H(i,j,k,\zeta_2^{-1},v,w)$$
$$= R\left[\frac{g^{p^2}-1}{\pi^i}, \frac{a_{\zeta_2^{-1}} g^p - 1}{\pi^j}, \frac{a_v b_w g - 1}{\pi^k}\right] \longrightarrow H(k) \to R.$$

Since the Hopf orders of Theorem 1.7 were constructed by a cohomology argument extending that in [Gr92], we shall call those Hopf orders *cohomological Hopf orders*.

The Hopf algebras in Theorem 1.7 are extensions of Larson orders by Larson duals, and involve five parameters: i, j, k, v and w. We can induce from them a collection of "6-parameter" triangular Hopf orders in KC_{p^3}.

Define ϱ' by

$$\begin{cases} \varrho' = i' + e' - \mathrm{ord}(\hat{u} - 1) \text{ if } \mathrm{ord}(\hat{u}-1) < i' + j, \\ \varrho' = j' \text{ if } \mathrm{ord}(\hat{u}-1) \geq i' + j \end{cases}$$

and ℓ by

$$\begin{cases} e'/p = \mathrm{ord}(\zeta_2 - 1) = i' + \ell \text{ if } e'/p < i' + \varrho, \\ \ell = \varrho \text{ if } e'/p \geq i' + \varrho. \end{cases}$$

Proposition 1.8. *Let $H(i,j,u)$ be a Hopf order with $i' \leq e'/p$. If $pk \leq \ell$ and v, w satisfy*

(A) $\mathrm{ord}(v-1) \geq i'/p + k$,
(B) $\mathrm{ord}(w-1) \geq \varrho'/p + k$,
(C) $\mathrm{ord}(w-1) \geq \varrho' + k/p$, *and*
(D) $\mathrm{ord}(v^p w^{-1} - 1) \geq pi' + k$,

then $H(i,\varrho,k,\zeta_2^{-1},v,w)$ is a cohomological Hopf order, and $H(i,j,k,u,v,w)$ is a triangular Hopf order.

Proof. To obtain $H(i,\varrho,k,\zeta_2^{-1},v,w)$ we need only check the inequalities

$$pi' \leq \varrho', \quad pk \leq \varrho$$

of Theorem 1.7. Since $e'/p \geq i'$, then by Lemma 1.6, $H(i,j,u)$ has a largest Larson dual,

$$\mathcal{LD}(A(i,j,u)) = H(\varrho', i')^* = H(i, \varrho, \zeta_2^{-1}),$$

where $\varrho' \geq pi'$ by construction. Then the assumption $pk \leq \ell$ implies that $pk \leq \varrho$ by definition of ℓ. Thus

$$H(i, \varrho, k, \zeta_2^{-1}, v, w) = H(i, j, \zeta_2^{-1}) \left[\frac{a_v b_w g - 1}{\pi^k} \right]$$

is a Hopf order. Since $H(i, \varrho, \zeta_2^{-1}) \subset H(i,j,u)$, it is clear that

$$H(i,j,k,u,v,w) = H(i,j,u) \left[\frac{a_v b_w g - 1}{\pi^k} \right]$$

is then a Hopf order, and there is an induced short exact sequence of Hopf orders

$$R \to H(i,j,u) \to H(i,j,k,u,v,w) \to H(k) \to R.$$

□

An R-Hopf order $H(i,j,k,u,v,w)$ arising in the manner of Proposition 1.8 will be called *a Hopf order induced from a Larson dual*, or, for short, an *ILD order*.

It is natural to ask whether all triangular Hopf orders are ILD orders as in Proposition 1.8. One goal in the remainder of this paper is to investigate this question. However, we shall soon show that under the restriction $e'/p \geq i'$, every triangular Hopf order is "induced from both ends" of an ILD Hopf order (Theorem 2.8).

2. Duality lemmas

In this section we collect together various results on duality needed in order to extend the construction of Theorem 1.2 to rank p^3 Hopf orders. We need two useful preliminary results.

Proposition 2.1. *If* $\mathrm{ord}(\hat{u} - 1) = i' + \nu' > 0$, $e' \geq \nu' \geq 0$, *then*

$$R \left[\frac{a_{\hat{u}} - 1}{\pi^{i'}} \right] = H(\nu).$$

Proof. We know that $a_{\hat{u}} - 1 \in \pi^{i'} H(\nu)$ by (1), hence

$$R \left[\frac{a_{\hat{u}} - 1}{\pi^{i'}} \right] \subset H(\nu).$$

To show equality, we compare discriminants. We have

$$\mathrm{disc}(H(\nu)) = \frac{p^p}{\pi^{p(p-1)\nu}} R$$

by [Gr92, Lemma 1.3a]. So

$$\mathrm{ord}(\mathrm{disc}(H(\nu)) = p(p-1)e' - p(p-1)\nu = p(p-1)\nu'.$$

On the other hand,

$$\begin{aligned}\operatorname{disc}\left(R\left[\frac{a_{\hat{u}}-1}{\pi^{i'}}\right]\right) &= \operatorname{disc}\left(1, \frac{a_{\hat{u}}-1}{\pi^{i'}}, \left(\frac{a_{\hat{u}}-1}{\pi^{i'}}\right)^2, \ldots, \left(\frac{a_{\hat{u}}-1}{\pi^{i'}}\right)^{p-1}\right) \\ &= \frac{1}{\pi^{i'p(p-1)}}\operatorname{disc}(1, a_{\hat{u}}-1, (a_{\hat{u}}-1)^2, \ldots, (a_{\hat{u}}-1)^{p-1}) \\ &= \frac{1}{\pi^{i'p(p-1)}}\operatorname{disc}(1, a_{\hat{u}}, a_{\hat{u}}^2, \ldots, a_{\hat{u}}^{p-1}).\end{aligned}$$

Now $a_{\hat{u}}^k = \sum_{\ell=0}^{p-1} \hat{u}^{\ell k} e_\ell$ for $k = 1, \ldots, p-1$. So

$$\begin{pmatrix} 1 \\ a_{\hat{u}} \\ a_{\hat{u}}^2 \\ \vdots \\ a_{\hat{u}}^{p-1} \end{pmatrix} = M \begin{pmatrix} e_0 \\ e_1 \\ e_2 \\ \vdots \\ e_{p-1} \end{pmatrix},$$

where

$$M = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \hat{u} & \hat{u}^2 & \ldots & \hat{u}^{p-1} \\ 1 & \hat{u}^2 & \hat{u}^4 & \ldots & \hat{u}^{2(p-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \hat{u}^{p-1} & \hat{u}^{2(p-1)} & \ldots & \hat{u}^{(p-1)^2} \end{pmatrix}.$$

Since

$$\operatorname{disc}(e_0, e_1, \ldots, e_{p-1}) = R,$$

it suffices to compute $(\det(M))^2$. Since M is Vandermonde,

$$\det(M) = \prod_{0 \le i < j \le p-1} (\hat{u}^j - \hat{u}^i).$$

But $\operatorname{ord}(\hat{u}^j - \hat{u}^i) = \operatorname{ord}(\hat{u}^{j-i} - 1) = \operatorname{ord}(\hat{u} - 1)$ since $\hat{u} \equiv 1 \bmod \pi R$. Thus

$$\operatorname{ord}(\det(M)) = \frac{p(p-1)}{2}\operatorname{ord}(\hat{u} - 1),$$

and so

$$\begin{aligned}\operatorname{ord}\left(\operatorname{disc} R\left[\frac{a_{\hat{u}}-1}{\pi^{i'}}\right]\right) &= (p-1)p(i'+\nu') - (p-1)pi' \\ &= (p-1)p\nu' \;=\; \operatorname{ord}(\operatorname{disc}(H(\nu)).\end{aligned}$$

Hence $R\left[\frac{a_{\hat{u}}-1}{\pi^{i'}}\right] = H(\nu)$, as we wished to prove. □

Corollary 2.2. a) *Let*

$$B = R\left[\frac{a_x - 1}{\pi^i}, \frac{a_y - 1}{\pi^j}\right].$$

If $\operatorname{ord}(x-1) = i + \mu' > 0$, $e' \ge \mu' \ge 0$ *and* $\operatorname{ord}(y-1) = j + \nu' > 0$, $e' \ge \nu' \ge 0$, *then* $B = H(max\{\mu, \nu\})$.

b) *If* $\operatorname{ord}(\hat{u}-1) = i' + \nu' > 0$, $e' \ge \nu' \ge 0$, $e' \ge j \ge 0$, *then*

$$R\left[\frac{a_{\hat{u}}-1}{\pi^{i'}}, \frac{\sigma - 1}{\pi^{j'}}\right] = H(\lambda)$$

with $\lambda = j'$ *if* $\nu < j'$, *and* $\lambda = \nu$ *if* $\nu \ge j'$.

Proof. Using Proposition 2.1, we have

$$\begin{aligned} B &= R\left[\frac{a_x-1}{\pi^i}\right]\left[\frac{a_y-1}{\pi^j}\right] \\ &= R\left[\frac{\sigma-1}{\pi^\mu}\right]\left[\frac{a_y-1}{\pi^j}\right] \\ &= R\left[\frac{a_y-1}{\pi^j}\right]\left[\frac{\sigma-1}{\pi^\mu}\right] \\ &= R\left[\frac{\sigma-1}{\pi^\nu}\right]\left[\frac{\sigma-1}{\pi^\mu}\right] \\ &= R\left[\frac{\sigma-1}{\pi^\lambda}\right], \end{aligned}$$

where $\lambda = max\{\mu,\nu\}$.

Statement b) follows easily from a) since $\sigma = a_{\zeta_1}$. □

In the next results we will use duality, and to keep track of which groups are involved, we shall subscript the duality brackets, as follows: $\langle\ ,\ \rangle_n$ will denote the duality map $KC_{p^n} \times K\hat{C}_{p^n} \to K$ for $n = 1, 2, 3$.

Our first duality results involve a "Gauss sum" defined in [GC98] that arises in duality computations.

Let x and y be any units in R. The quantity

$$G(x,y) = \frac{1}{p}\sum_{0\le i,j\le p-1} \zeta_1^{-ij}x^iy^j$$

is defined to be the *Gauss sum of x and y* ([GC98]). Note that $G(x,1) = 1$. Also,

$$\begin{aligned} G(\zeta_1^k, w) &= \frac{1}{p}\sum_{i,j=0}^{p-1} \zeta_1^{ki}\zeta_1^{-ij}w^j \\ &= \frac{1}{p}\sum_{j=0}^{p-1}(\sum_{i=0}^{p-1}\zeta_1^{(k-j)i})w^j = w^k. \end{aligned}$$

The Gauss sum arises in connection with duality because

$$G(x,y) = \langle a_x, a_y\rangle$$

(where $a_x \in KC_p$, $a_y \in K\hat{C}_p$), as is easily verified (cf. [GC98]).

Proposition 2.3. *Let x, y be units in R with $e' > \mathrm{ord}(1-x)$, $e' > \mathrm{ord}(1-y)$, and $\mathrm{ord}(1-x) + \mathrm{ord}(1-y) > e'$. Then*

$$\mathrm{ord}(G(x,y)-1) = \mathrm{ord}(\langle a_x, a_y\rangle_1 - 1) = \mathrm{ord}(1-x) + \mathrm{ord}(1-y) - e'.$$

Proof. Let $\mathrm{ord}(1-x) = n$ and $\mathrm{ord}(1-y) = n' + s$, and suppose

$$\mathrm{ord}(\langle a_x, a_y\rangle_1 - 1) = \mathrm{ord}(\langle a_x - 1, a_y - 1\rangle_1) = t.$$

We have $a_x - 1 \in H(n')$, and $a_y - 1 \in \pi^s H(n)$ by (1). Thus

$$\langle a_x - 1, a_y - 1\rangle_1 \in \pi^s R,$$

hence $t \geq s$. Now

$$\begin{aligned}\langle (a_x-1)^2, a_y-1\rangle_1 &= \langle (a_x-1)^2, a_y\rangle_1 \\ &= (\langle a_x-1, a_y\rangle_1)^2 + \langle (a_x-1)\otimes(a_x-1), \Delta\rangle_1 \\ &= (\langle a_x-1, a_y-1\rangle_1)^2 + \langle (a_x-1)\otimes(a_x-1), \Delta\rangle_1,\end{aligned}$$

where

$$\Delta = \Delta(a_y) - a_y \otimes a_y \in \pi^{ps} H(n) \otimes H(n)$$

since $\mathrm{ord}(y^p - 1) = pn' + ps$ [C00, (31.10)]. So

$$\mathrm{ord}(\langle (a_x-1)^2, a_y-1\rangle_1) \geq min\{2t, ps\}.$$

Then

$$\begin{aligned}&\langle (a_x-1)^3, a_y-1\rangle_1 \\ &\qquad = \langle (a_x-1)^2, a_y\rangle_1 \langle a_x-1, a_y\rangle_1 + \langle (a_x-1)^2 \otimes (a_x-1), \Delta\rangle_1\end{aligned}$$

has order $\geq min\{3t, ps\}$, etc. So

$$\left\langle R[a_x-1], \frac{\hat{a}_y - 1}{\pi^q} \right\rangle_1 \in R,$$

where $q = \min\{t, ps\} \geq s$. But $R[a_x - 1] = H(n')$ by Proposition 2.1. Hence $\frac{\hat{a}_y - 1}{\pi^q} \in H(n)$. Thus $\mathrm{ord}(y-1) \geq n' + q$ by (1). Since $q \geq s$ and $\mathrm{ord}(y-1) = n' + s$, we have $s = t = q$. That completes the proof. □

Lemma 2.4. *Suppose* $e' > \mathrm{ord}(1-x_i)$, $e' > \mathrm{ord}(1-y)$, *and* $\mathrm{ord}(1-x_i) + \mathrm{ord}(1-y) \geq e' + s$, $s \geq 0$, $i = 1, 2$. *Then*

$$G(x_1x_2, y) \equiv G(x_1, y)G(x_2, y) \pmod{\pi^{ps}R}.$$

Proof.

$$\begin{aligned}G(x_1, y)G(x_2, y) - G(x_1x_2, y) &= \langle a_{x_1}, a_y\rangle_1 \langle a_{x_2}, a_y\rangle_1 - \langle a_{x_1}a_{x_2}, a_y\rangle_1 \\ &= \langle a_{x_1} \otimes a_{x_2}, a_y \otimes a_y\rangle_1 - \langle a_{x_1} \otimes a_{x_2}, \Delta(a_y)\rangle_1 \\ &= \langle a_{x_1} \otimes a_{x_2}, a_y \otimes a_y - \Delta(a_y)\rangle_1.\end{aligned}$$

Let $\mathrm{ord}(1-y) = n' + s$. Then $\mathrm{ord}(1-x_i) \geq n$, so $a_{x_i} \in H(n'), i = 1, 2$, and

$$a_y \otimes a_y - \Delta(a_y) \in \pi^{ps} H(n) \otimes H(n).$$

Thus

$$\langle a_{x_1} \otimes a_{x_2}, a_y \otimes a_y - \Delta(a_y)\rangle_1 \in \pi^{ps} R.$$

□

Corollary 2.5. *Suppose* $e' > \mathrm{ord}(1-x) \geq n$ *and* $e' > \mathrm{ord}(1-y) \geq n' + s$, $s \geq 0$. *Then for* $0 \leq m \leq p-1$,

$$G(x, y)^m \equiv G(x^m, y) \pmod{\pi^{ps}R}$$

and

$$G(x\zeta_1^m, y) \equiv G(x, y)y^m \pmod{\pi^{ps}R}.$$

Proof. The first formula is an easy induction. The second is an immediate consequence of the property that $G(\zeta_1^m, y) = y^m$. □

Lemma 2.6 (Reduction Lemma)**.** *Let v be an element of K, and let τ be the generator of $\hat{C}_{p^2}$ for which $\langle g^p, \tau\rangle_2 = \zeta_2$. Then for all $0 \le c, d \le p-1$,*

$$\langle b_y, a_v\tau^{pc+d}\rangle_2 = G(v\zeta_1^c, y) = \langle a_v a_{\zeta_1}^c, a_y\rangle_1.$$

Proof.

$$\begin{aligned}
\langle b_y, a_v\tau^{pc+d}\rangle_2 &= \left\langle \sum_{m,n=0}^{p-1} y^m e^2_{pm+n}, a_v\tau^{pc+d}\right\rangle_2 \\
&= \left\langle \sum_{m,n=0}^{p-1} y^m e^2_{pm+n}, \sum_{q=0}^{p-1} v^q e^1_q \tau^{pc+d}\right\rangle_2 \\
&= \left\langle \sum_{m,n=0}^{p-1} y^m e^2_{pm+n}, \sum_{q=0}^{p-1} v^q \frac{1}{p}\sum_{r=0}^{p-1} \zeta_1^{-qr}\tau^{pr+pc+d}\right\rangle_2 \\
&= \frac{1}{p}\sum_{m,n,q,r=0}^{p-1} v^q y^m \zeta_1^{-qr}\langle e^2_{pm+n}, \tau^{pr+pc+d}\rangle_2.
\end{aligned}$$

Note that $\langle e^2_{pm+n}, \tau^{pr+pc+d}\rangle_2 = 1$ if $n = d$ and $m \equiv r+c \bmod p$, that is, if $r \equiv m-c$, and $\langle e^2_{pm+n}, \tau^{pr+pc+d}\rangle_2 = 0$ in all other cases. Thus

$$\begin{aligned}
\langle b_y, a_v\tau^{pc+d}\rangle_2 &= \frac{1}{p}\sum_{m,q=0}^{p-1} v^q\zeta_1^{-q(m-c)} y^m \\
&= \frac{1}{p}\sum_{m,q=0}^{p-1} (v\zeta_1^c)^q \zeta_1^{-qm} y^m \\
&= G(v\zeta_1^c, y) \\
&= \langle a_v a_{\zeta_1^c}, a_y\rangle_1.
\end{aligned}$$

□

Using the Reduction Lemma, we can study when $b_y - 1$ is in $\pi^q A(i,j,u)$, where $A(i,j,u)$ is an arbitrary R-Hopf order in KC_{p^2}.

Theorem 2.7. a) *Let y be a unit of R. Suppose $A(i,j,u)$ is a Hopf order and let $\hat{u} = \zeta_2^{-1}u^{-1}$ with $\operatorname{ord}(\hat{u}-1) = i' + \nu' > 0$ with $e' \ge \nu' \ge 0$. Then $b_y - 1$ is in $\pi^q A(i,j,u)$ iff $\operatorname{ord}(y-1) \ge \varrho' + q$, where*

$$\varrho' = \nu \text{ if } \nu' < j \text{ and}$$
$$\varrho' = j' \text{ if } \nu' \ge j.$$

b) *Suppose $\operatorname{ord}(y-1) < e'$. Then $b_y - 1 \in \pi^q A(i,j,u)$ if and only if $\operatorname{ord}(\hat{u}-1) \ge i'$ and $\operatorname{ord}(y-1) \ge \varrho' + q$.*

Proof. We have $b_y - 1 \in \pi^q A(i,j,u)$ iff

$$\langle b_y - 1, (\tau^p - 1)^r (a_{\hat{u}}\tau - 1)^s\rangle_2 \in \pi^{q + rj' + si'} R, \tag{3}$$

for $0 \le r, s \le p-1$. If $r = s = 0$, we have

$$\langle b_y - 1, (\tau^p - 1)^r (a_{\hat{u}}\tau - 1)^s\rangle_2 = \langle b_y - 1, 1\rangle_2 = 0,$$

so (3) holds iff

$$\langle b_y - 1, (\tau^p - 1)^r (a_{\hat{u}}\tau - 1)^s \rangle_2 \in \pi^{q+rj'+si'} R$$

for $0 < r + s$. Since

$$\langle 1, (\tau^p - 1)^r (a_{\hat{u}}\tau - 1)^s \rangle_2 = 0$$

for $r + s > 0$, we have for $r + s > 0$,

$$\begin{aligned}
&\langle b_y - 1, (\tau^p - 1)^r (a_{\hat{u}}\tau - 1)^s \rangle_2 \\
&\quad = \langle b_y, (\tau^p - 1)^r (a_{\hat{u}}\tau - 1)^s \rangle_2 \\
&\quad = \sum_{c=0}^{r} \sum_{d=0}^{s} \binom{r}{c} \binom{s}{d} (-1)^{r-c} (-1)^{s-d} \langle b_y, \tau^{pc} (a_{\hat{u}}\tau)^d \rangle_2 \\
&\quad = \sum_{c=0}^{r} \sum_{d=0}^{s} \binom{r}{c} \binom{s}{d} (-1)^{r-c} (-1)^{s-d} \langle a_{\hat{u}}^d a_{\zeta_1}^c, a_y \rangle_1, \\
&\qquad \text{(by the Reduction Lemma 2.6)} \\
&\quad = \langle (a_{\hat{u}} - 1)^s (a_{\zeta_1} - 1)^r, a_y \rangle_1.
\end{aligned}$$

Thus condition (3) is equivalent to the condition

$$\langle (a_{\hat{u}} - 1)^s (a_{\zeta_1} - 1)^r, a_y \rangle_1 \in \pi^{q+rj'+si'} R$$

or

$$\left\langle \left(\frac{a_{\hat{u}} - 1}{\pi^{i'}} \right)^s \left(\frac{a_{\zeta_1} - 1}{\pi^{j'}} \right)^r, a_y \right\rangle_1 = \left\langle \left(\frac{a_{\hat{u}} - 1}{\pi^{i'}} \right)^s \left(\frac{\sigma - 1}{\pi^{j'}} \right)^r, a_y \right\rangle_1 \in \pi^q R,$$

where $\sigma = g^{p^2}$ and $0 \le r, s \le p - 1$, $0 < r + s$. Since for all $0 \le r, s \le p - 1$ with $0 < r + s$, we have

$$\left\langle \left(\frac{a_{\hat{u}} - 1}{\pi^{i'}} \right)^s \left(\frac{\sigma - 1}{\pi^{j'}} \right)^r, 1 \right\rangle_1 = 0,$$

and since $\langle 1, a_{y^p} - 1 \rangle = 0$, (3) is equivalent to

$$\left\langle \left(\frac{a_{\hat{u}} - 1}{\pi^{i'}} \right)^s \left(\frac{\sigma - 1}{\pi^{j'}} \right)^r, a_y - 1 \right\rangle_1 \in \pi^q R \tag{4}$$

for all $0 \le r, s \le p - 1$. Assume $\operatorname{ord}(\hat{u} - 1) = i' + \nu' > 0$, $e' \ge \nu' \ge 0$. Then by Corollary 2.2b),

$$R \left[\frac{a_{\hat{u}} - 1}{\pi^{i'}}, \frac{\sigma - 1}{\pi^{j'}} \right] = H(\varrho')$$

for $\varrho' = \nu$ if $\nu' < j$, and $\varrho' = j'$ if $\nu' \ge j$. Thus (4) is equivalent to $a_y - 1 \in \pi^q H(\varrho)$, which by (1) is equivalent to $\operatorname{ord}(y - 1) \ge \varrho' + q$, giving a).

For b): It suffices to show, assuming $\operatorname{ord}(y-1) < e'$, that if $b_y - 1$ is in $\pi^q A(i, j, u)$, then $\operatorname{ord}(\hat{u} - 1) = i' + \nu' \ge i'$ and $\operatorname{ord}(y - 1) \ge j' + q \ge \varrho' + q$.

Since $b_y - 1$ is in $\pi^q A(i, j, u)$, then for all $0 \le r, s \le p - 1$ with $r + s > 0$,

$$\langle (a_{\hat{u}} - 1)^s (\sigma - 1)^r, a_y \rangle \in \pi^{q+si'+rj'} R.$$

In particular, for $s = 0, r = 1$ we have

$$y - 1 = \langle \sigma - 1, a_y \rangle \in \pi^{q+j'} R,$$

hence $\operatorname{ord}(y - 1) \ge j' + q$. Also, for $s = 1, r = 0$ we have

$$\langle a_{\hat{u}} - 1, a_y \rangle = G(\hat{u}, y) - 1 \in \pi^{q+i'} R.$$

Since $A(i,j,u)$ is a Hopf order, by Theorem 1.5 we have $\operatorname{ord}(\hat{u}-1) \geq i'/p + j$. Hence

$$\operatorname{ord}(\hat{u}-1) + \operatorname{ord}(y-1) \geq j' + q + i'/p + j > e'.$$

Assume $\operatorname{ord}(y-1) < e'$. If $\operatorname{ord}(\hat{u}-1) \geq e'$, then $\operatorname{ord}(\hat{u}-1) \geq i'$. Otherwise, by Proposition 2.3,

$$\operatorname{ord}(G(\hat{u},y)-1) + e' = \operatorname{ord}(y-1) + \operatorname{ord}(\hat{u}-1),$$

hence

$$\operatorname{ord}(y-1) + \operatorname{ord}(\hat{u}-1) \geq e' + i' + q.$$

Since $\operatorname{ord}(y-1) < e'$, we have $\operatorname{ord}(\hat{u}-1) \geq i' + q \geq i'$. Since $\varrho' \leq j'$ we have $\operatorname{ord}(y-1) \geq j' + q \geq \varrho' + q$, proving b). □

Using Theorem 2.7 one can show that if $e'/p \geq i'$, then every triangular Hopf order is induced from "both ends" of an ILD Hopf order.

Theorem 2.8. *Let $H = A(i,j,u)\left[\frac{a_v b_w g - 1}{\pi^k}\right]$ be a triangular Hopf order with $e'/p \geq i'$ and a_v, b_w elements of $A(i,j,u)$, $v, w \in U(R)$. Then there exists $\mu \leq k$ so that*

$$H' = A(i,j,u)\left[\frac{a_v b_w g - 1}{\pi^\mu}\right]$$

is an ILD order.

Proof. If $e'/p \geq i'$, then $\operatorname{ord}(\hat{u}-1) \geq i'$: referring to Remark 1.4, this is clear in cases (1) and (2), where $\operatorname{ord}(\hat{u}-1) \geq i'$; in case (3), $\operatorname{ord}(\hat{u}-1) = \operatorname{ord}(u-1) \geq i' + j/p$. Now since $a_v \in A(i,j,u)$, we have $a_v \in H(i)$, hence by (1), $\operatorname{ord}(v-1) \geq i'$. Now by Theorem 2.7a), since $b_w \in A(i,j,u)$, we have $\operatorname{ord}(w-1) \geq \varrho'$, where $\varrho' = j'$ if $\operatorname{ord}(\hat{u}-1) \geq i' + j$, and otherwise $\operatorname{ord}(\hat{u}-1) = i' + \varrho$. The largest Larson dual in $A(i,j,u)$ is $H(\varrho', i')^*$, and $\varrho' \geq pi'$. We show that for some $\mu \leq k$, the triangular Hopf order

$$H_0 = H(\varrho', i')^*\left[\frac{a_v b_w g - 1}{\pi^\mu}\right]$$

satisfies the conditions of Theorem 1.7, namely:

(A) $\operatorname{ord}(v-1) \geq i'/p + \mu$;
(B) $\operatorname{ord}(w-1) \geq \varrho'/p + \mu$;
(C) $\operatorname{ord}(w-1) \geq \varrho' + \mu/p$;
(D) $\operatorname{ord}(v^p w^{-1} - 1) \geq pi' + \mu$,

with $p\mu \leq l$, $H(i,l) = \mathcal{L}(H(\varrho', i')^*)$.

Since $\operatorname{ord}(v-1) \geq i'$ and $\varrho' \geq pi'$, we have

$$\operatorname{ord}(v^p w^{-1} - 1) \geq min\{\operatorname{ord}(v^p - 1), \operatorname{ord}(w-1)\} \geq pi'.$$

So let

$$\operatorname{ord}(v^p w^{-1} - 1) = pi' + \mu_D.$$

Since $\operatorname{ord}(w-1) \geq \varrho'/p$, let

$$\operatorname{ord}(w-1) = \varrho'/p + \mu_B = \varrho' + \mu_C/p.$$

Since $\operatorname{ord}(v-1) \geq i'$, let $\operatorname{ord}(v-1) = i'/p + \mu_A$. Finally, let μ satisfy

$$0 \leq \mu \leq min\{k, \mu_A, \mu_B, \mu_C, \mu_D, l/p\}.$$

Then $p\mu \leq l$ and all of the inequalities (A)–(D) hold, so H' is an ILD Hopf order. □

3. Duality Hopf orders

We begin this section by isolating the main idea of Theorem 1.2.

Theorem 3.1. *Let K contain a primitive p^nth root of unity. Let G be cyclic of order p^n with character group $\hat{G}$. Suppose H is an order over R in KG and J is an order over R in $K\hat{G}$. If $\langle J, H\rangle \subset R$ and $disc(H^*) = disc(J)$, then $J = H^*$ and both are Hopf orders.*

Proof. It is well known that the two hypotheses,

$$\langle J, H\rangle \subset R \text{ and } disc(H^*) = disc(J),$$

imply that $J = H^*$. But if $J = H^*$ and J is an order over R in $K\hat{G} = KG^*$, hence an R-algebra with operations induced from KG^*, then $J^* = H$ is an R-coalgebra with operations induced from KG, and hence H is a bialgebra. Since H is also closed under the inverse map, H is a Hopf order. Then $H^* = J$ is also a Hopf order. □

Using Theorem 3.1 we will construct triangular Hopf orders using a duality argument, a generalization to Hopf orders in KC_{p^3} of the construction we presented for KC_{p^2} as Theorem 1.2. Before doing so, we note some lemmas:

Lemma 3.2. *Let $i' > 0$. Then a_u is a unit of $H(i)$ iff $u - 1 \in \pi^{i'}R$.*

Proof. We have a_u in $H(i)$ iff $a_u - 1 \in H(i)$, iff $u - 1 \in \pi^{i'}R$ by (1). But then u is a unit of R and $u^{-1} - 1 \in \pi^{i'}R$, so $a_{u^{-1}} \in H(i)$, and $a_u a_{u^{-1}} = a_1 = 1$. □

Lemma 3.3. *If $q \le e'$, then for x in R,* $\mathrm{ord}(x^p - 1) \ge pq$ *if and only if* $\mathrm{ord}(x-1) \ge q$.

Proof. If $\mathrm{ord}(x - 1) \ge q$, $q \le e'$, then $\mathrm{ord}((1 - x)^p) \ge pq$. By the binomial theorem, $(x - 1)^p = x^p - 1 + W$, where W is so that $\mathrm{ord}(W) = e + q$. Now if $e + q > \mathrm{ord}(x^p - 1)$, then $\mathrm{ord}(x^p - 1) \ge pq$. Otherwise, if $e + q \le \mathrm{ord}(x^p - 1)$, then $\mathrm{ord}(x^p - 1) \ge pq$ since $e' \ge q$. Conversely, suppose $\mathrm{ord}(x^p - 1) \ge pq$, $e' \ge q$. If $e + q \ge \mathrm{ord}(x^p - 1)$, then $\mathrm{ord}(x - 1) \ge q$. On the other hand, if $e + q < \mathrm{ord}(x^p - 1)$, then $\mathrm{ord}((x - 1)^p) \ge e + q \ge pq$, hence $\mathrm{ord}(x - 1) \ge q$. □

The next lemma is a routine computation, analogous to Lemma 1.3, using the fundamental duality relation $\langle g^m, \gamma^n\rangle_3 = \zeta_3^{mn}$.

Lemma 3.4. *Let $G = C_{p^3} = \langle g\rangle$, $\hat{G} = \langle\gamma\rangle$, and let e^2_{pa+b}, $\hat{e}^2_{pm+n}$, $a, b, m, n = 0, \ldots, p - 1$, denote the idempotents in the maximal integral orders in $K[g^p]$ and $K[\gamma^p]$, respectively. Then for all $0 \le c, d, e, \alpha, \beta, \delta \le p - 1$,*

$$\langle e_{pa+b} g^{p^2c+pd+e}, \hat{e}_{pm+n}\gamma^{p^2\alpha+p\beta+\delta}\rangle_3 = \frac{1}{p}\zeta_1^{-(m-d)(a-\beta)}\zeta_3^{(p^2c+pd+e)(p^2\alpha+p\beta+\delta)},$$

if $n = e$ and $b = \delta$, and 0 in all other cases.

Assume that K contains ζ_3, a primitive p^3rd root of unity. Let γ generate $\hat{C}_{p^3}$, the character group of C_{p^3}, so that $\langle\gamma, g\rangle_3 = \zeta_3$. To begin the duality construction, let $A = A(i, j, u)$, $i' > 0$, be an R-Hopf order in $K\langle g^p\rangle$, and for $v, w \in U(R)$, let

$$H = A(i, j, k, u, v, w) = A\left[\frac{a_v b_w g - 1}{\pi^k}\right],$$

where, recall,

$$a_v b_w = \sum_{l=0}^{p-1} v^l e_l^1 \cdot \sum_{m,n=0}^{p-1} w^m e_{pm+n}^2 = \sum_{m,n=0}^{p-1} v^n w^m e_{pm+n}^2.$$

Let $B = A(k', j', z)$, $k > 0$, be an R-Hopf order in $K\langle\gamma^p\rangle$, and let

$$J = A(k', j', i', z, x, y) = B\left[\frac{a_x b_y \gamma - 1}{\pi^{i'}}\right],$$

where $x, y \in U(R)$. We note that if H is a Hopf order, then both $A(i, j, u)$ and $A(j, k, w)$, the image of H under the map sending g^{p^2} to 1, are Hopf orders, and hence necessarily $i \geq j \geq k$ (cf. Remark 1.4). So we assume $i \geq j \geq k$.

We wish to find conditions on u, v, w, x, y, z in order that H and J are R-algebras and $\langle H, J\rangle_3 \subset R$. Once we do so, then since the discriminants of H and J depend only on i, j, k (cf. the proof of Theorem 1.2), it is routine to see that $\operatorname{disc}(J) = \operatorname{disc}(H^*)$ and so $J = H^*$.

First we find conditions for H to be an R-order. For this we want

- A is a Hopf order, free of rank p over the Larson order $H(i)$.

By Theorem 1.2 this is true if a_u is a unit of $H(i)$, which is equivalent to

- $u - 1 \in \pi^{i'} R$, by Lemma 3.2; and also
- $u^p - 1 \in \pi^{pi'+j} R$; and
- $u^p \zeta_1 - 1 \in \pi^{i'+pj} R$.

If $u^p - 1 \in \pi^{pi'+j} R$, then since $j \leq i$, Lemma 3.3 gives $\operatorname{ord}(u-1) \geq i' + j/p$, hence $u - 1 \in \pi^{i'} R$ follows from the other conditions.

- H is an R-algebra, free of rank p over A.

By [C00, (31.1)], this is true iff $(a_v b_w)^p g^p - 1 \in \pi^{pk} A(i, j, u)$. Note that

$$\begin{aligned}(a_v b_w g)^p &= a_{v^p} b_{w^p} g^p \\ &= \sum_{a,b=0}^{p-1} (v^p)^b (w^p)^a e_{pa+b} g^p \\ &= \sum_{a,b=0}^{p-1} (v^p)^b (w^p)^a \zeta_2^{pa+b} e_{pa+b} \\ &= a_{v^p \zeta_2} b_{w^p \zeta_1}.\end{aligned}$$

Then $a_{v^p\zeta_2} b_{w^p\zeta_1} - 1 \in \pi^{pk} A(i, j, u)$ if

$$a_{v^p\zeta_2} - 1 \in \pi^{pk} H(i)$$

and

$$b_{w^p\zeta_1} - 1 \in \pi^{pk} A(i, j, u).$$

The first holds iff

$$\operatorname{ord}(v^p\zeta_2 - 1) \geq i' + pk,$$

and if $\operatorname{ord}(\hat{u} - 1) \geq i'$, the second holds iff

$$\operatorname{ord}(w^p\zeta_1 - 1) + \operatorname{ord}(\hat{u} - 1) \geq i' + e' + pk \text{ if } \operatorname{ord}(\hat{u} - 1) < i' + j,$$
$$\operatorname{ord}(w^p\zeta_1 - 1) \geq j' + pk \text{ if } \operatorname{ord}(\hat{u} - 1) \geq i' + j$$

by Theorem 2.7a).

We collect these conditions into

Proposition 3.5. *The algebra*

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

is free of rank p over the Hopf order $A(i,j,u)$ if $i \geq j \geq k$ and the following inequalities hold:

(i) $\operatorname{ord}(u-1) \geq i' + j/p$;
(ii) $\operatorname{ord}(\hat{u}-1) \geq i'/p + j$;
(iii) $\operatorname{ord}(v^p\zeta_2 - 1) \geq i' + pk$;
(iv) $\operatorname{ord}(\hat{u}-1) \geq i' > 0$;
(v) $\operatorname{ord}(w\zeta_2 - 1) \geq j'/p + k$;
(vi) $\operatorname{ord}(\hat{u}-1) + \operatorname{ord}(w^p\zeta_1 - 1) \geq e' + i' + pk$.

Similarly, we have

Proposition 3.6. *The algebra*

$$J = A(k',j',i',z,x,y) = R\left[\frac{g^{p^2}-1}{\pi^{k'}}, \frac{a_z g^p - 1}{\pi^{j'}}, \frac{a_x b_y g - 1}{\pi^{i'}}\right]$$

is free of rank p over the Hopf order $A(k',j',z)$ if $k' \geq j' \geq i'$ and the following inequalities hold:

(i) $\operatorname{ord}(z-1) \geq k + j'/p$;
(ii) $\operatorname{ord}(\hat{z}-1) \geq k/p + j'$;
(iii) $\operatorname{ord}(x^p\zeta_2 - 1) \geq k + pi'$;
(iv) $\operatorname{ord}(\hat{z}-1) \geq k > 0$;
(v) $\operatorname{ord}(y\zeta_2 - 1) \geq j/p + i'$;
(vi) $\operatorname{ord}(\hat{z}-1) + \operatorname{ord}(y^p\zeta_1 - 1) \geq e' + k + pi'$.

We are left with choosing relations among u,v,w,x,y,z and conditions so that $\langle J, H\rangle \subset R$. Here is the result.

Theorem 3.7. *Suppose $i \geq j \geq k$. Consider the following valuation inequalities:*

(i) $e' > \operatorname{ord}(\hat{u}-1) \geq i'/p + j$;
(ii) $\operatorname{ord}(v^p\zeta_2 - 1) \geq i' + pk$;
(iii) $\operatorname{ord}(\hat{u}-1) \geq i' > 0$;
(iv) $\operatorname{ord}(\hat{u}-1) + \operatorname{ord}(w^p\zeta_1 - 1) \geq e' + i' + pk$;
(v) $\operatorname{ord}(w\zeta_2 - 1) = \operatorname{ord}(z-1) \geq j'/p + k$;
(vi) $\operatorname{ord}(u-1) = \operatorname{ord}(\hat{y}-1) \geq i' + j/p$;
(vii) $e' > \operatorname{ord}(\hat{z}-1) \geq k/p + j'$;
(viii) $\operatorname{ord}(x^p\zeta_2 - 1) \geq k + pi'$;
(ix) $\operatorname{ord}(\hat{z}-1) \geq k > 0$;
(x) $\operatorname{ord}(\hat{z}-1) + \operatorname{ord}(y^p\zeta_1 - 1) \geq e' + k + pi'$; *and*
(xi) $\operatorname{ord}(\hat{z}-1) + \operatorname{ord}(\hat{u}-1) \geq e' + (\frac{p-1}{p})(i' + k + e')$.

Then $H = A(i,j,k,u,v,w)$ is an R-algebra, free over the R-Hopf order $A(i,j,u)$, if inequalities (i)–(vi) *hold; $J = A(k',j',i',z,x,y)$ is an R-algebra, free over the R-Hopf order $A(k',j',z)$, if inequalities* (v)–(x) *hold;, and H and J are dual triangular Hopf orders in KC_{p^3} if $\hat{z} = w, \hat{u} = y$, $vx\zeta_3 G(\hat{u},\hat{z}) = 1$ and inequality* (xi) *holds.*

Proof. Since it is easy to verify that H and J are closed under the antipode (inverse) map on KG, to finish the proof we need to show that $\langle J, H\rangle \subset R$. To do this, we require that

$$\begin{aligned}\operatorname{ord}(\langle (g^{p^2}-1)^q(a_u g^p-1)^r(a_v b_w g-1)^s, (\gamma^{p^2}-1)^\sigma(a_z\gamma^p-1)^\tau(a_x b_y\gamma-1)^\varepsilon\rangle_3)\\ \geq qi+rj+sk+\sigma k'+\tau j'+\varepsilon i',\end{aligned}$$

for $q, r, s, \sigma, \tau, \varepsilon = 0, \ldots, p-1$. Put

$$\eta = \langle (g^{p^2}-1)^q(a_u g^p-1)^r(a_v b_w g-1)^s, (\gamma^{p^2}-1)^\sigma(a_z\gamma^p-1)^\tau(a_x b_y\gamma-1)^\varepsilon\rangle_3.$$

Then

$$\begin{aligned}\eta &= \sum_{c,d,e,\alpha,\beta,\delta=0}^{q,r,s,\sigma,\tau,\varepsilon} C\langle g^{p^2 c}a_{u^d}g^{pd}a_{v^e}b_{w^e}g^e, \gamma^{p^2\alpha}a_{z^\beta}\gamma^{p\beta}a_{x^\delta}b_{y^\delta}\gamma^\delta\rangle_3\\ &= \sum_{c,d,e,\alpha,\beta,\delta=0}^{q,r,s,\sigma,\tau,\varepsilon} C\langle g^{p^2c+pd+e}a_{u^d v^e}b_{w^e}, \gamma^{p^2\alpha+p\beta+\delta}a_{z^\beta x^\delta}b_{y^\delta}\rangle_3\\ &= \sum_{c,d,e,\alpha,\beta,\delta=0}^{q,r,s,\sigma,\tau,\varepsilon} C(c,d,e,\alpha,\beta,\delta)\Gamma,\end{aligned}$$

where

$$\begin{aligned}C &= C(c,d,e,\alpha,\beta,\delta)\\ &= \binom{q}{c}\binom{r}{d}\binom{s}{e}\binom{\sigma}{\alpha}\binom{\tau}{\beta}\binom{\varepsilon}{\delta}(-1)^{q-c}(-1)^{r-d}(-1)^{s-e}(-1)^{\sigma-\alpha}(-1)^{\tau-\beta}(-1)^{\varepsilon-\delta}\end{aligned}$$

and

$$\Gamma = \sum_{pa+b,pm+n=0}^{p^2-1} u^{db}v^{eb}w^{ae}z^{\beta n}x^{\delta n}y^{m\delta}\langle e_{pa+b}g^{p^2c+pd+e}, \hat{e}_{pm+n}\gamma^{p^2\alpha+p\beta+\delta}\rangle_3.$$

By Lemma 3.4,

$$\langle e_{pa+b}g^{p^2c+pd+e}, \hat{e}_{pm+n}\gamma^{p^2\alpha+p\beta+\delta}\rangle_3 = \frac{1}{p}\zeta_1^{-(m-d)(a-\beta)}\zeta_3^{(p^2c+pd+e)(p^2\alpha+p\beta+\delta)}\delta_{e,n}\delta_{b,\delta}$$

so since $uy\zeta_2 = 1 = wz\zeta_2$ and $vx\zeta_3 G(w,y) = 1$, we have

$$\begin{aligned}\Gamma &= \frac{1}{p}\sum_{a,m=0}^{p-1} u^{d\delta}v^{e\delta}w^{ae}z^{\beta e}x^{\delta e}y^{m\delta}\zeta_1^{-(m-d)(a-\beta)}\zeta_3^{(p^2c+pd+e)(p^2\alpha+p\beta+\delta)}\\ &= u^{d\delta}\zeta_2^{d\delta}z^{\beta e}\zeta_2^{\beta e}(vx\zeta_3)^{e\delta}\zeta_1^{c\delta+d\beta+e\alpha}\frac{1}{p}\sum_{a,m=0}^{p-1} y^{m\delta}w^{ae}\zeta_1^{-(m-d)(a-\beta)}\\ &= y^{-d\delta}w^{-\beta e}(vx\zeta_3)^{e\delta}\zeta_1^{c\delta+e\alpha}\frac{1}{p}\sum_{a,m=0}^{p-1}(y^\delta\zeta_1^\beta)^m\zeta_1^{-am}(w^e\zeta_1^d)^a\\ &= y^{-d\delta}w^{-\beta e}(vx\zeta_3)^{e\delta}\zeta_1^{c\delta+e\alpha}G(y^\delta\zeta_1^\beta, w^e\zeta_1^d)\\ &= y^{-d\delta}w^{-\beta e}G(y,w)^{-e\delta}\zeta_1^{c\delta+e\alpha}G(y^\delta\zeta_1^\beta, w^e\zeta_1^d).\end{aligned}$$

Now, by (i), $e' > \operatorname{ord}(1-y)$ and by (vii), $e' > \operatorname{ord}(w-1)$. Moreover, $\operatorname{ord}(w-1) + \operatorname{ord}(y-1) \geq e'+f$, with $f = (\frac{p-1}{p})(i'+k+e') \geq 0$ by (xi). Thus, Corollary 2.5

yields

$$\begin{aligned} G(y^\delta\zeta_1^\beta, w^e\zeta_1^d) &\equiv G(y^\delta, w^e\zeta_1^d)(w^e\zeta_1^d)^\beta \\ &\equiv G(y^\delta, w^e)y^{d\delta}w^{e\beta}\zeta_1^{d\beta} \pmod{\pi^{pf}R} \\ &= G(y,w)^{e\delta}y^{d\delta}w^{e\beta}\zeta_1^{d\beta} + \pi^{pf}m_{\delta,\beta,e,d}, \end{aligned}$$

where $m_{\delta,\beta,e,d}$ is in R. So

$$\Gamma = \zeta_1^{c\delta+e\alpha+d\beta}(1+\pi^{pf}n_{\delta,\beta,e,d}),$$

for some element $n_{\delta,\beta,e,d}$ in R. Then

$$\begin{aligned} \eta &= \sum_{c,d,e,\alpha,\beta,\delta=0}^{q,r,s,\sigma,\tau,\varepsilon} C\Gamma \\ &= \sum_{c,d,e,\alpha,\beta,\delta=0}^{q,r,s,\sigma,\tau,\varepsilon} C(1+\pi^{pf}n_{\delta,\beta,e,d})\zeta_1^{c\delta+e\alpha+d\beta} \\ &= \sum_{c,d,e,\alpha,\beta,\delta=0}^{q,r,s,\sigma,\tau,\varepsilon} C\zeta_1^{c\delta+e\alpha+d\beta} \\ &\quad + \pi^{pf}\sum_{c,d,e,\alpha,\beta,\delta=0}^{q,r,s,\sigma,\tau,\varepsilon} Cn_{\delta,\beta,e,d}\zeta_1^{c\delta+e\alpha+d\beta}. \end{aligned}$$

Now the first sum

$$\sum_{c,d,e,\alpha,\beta,\delta=0}^{q,r,s,\sigma,\tau,\varepsilon} C\zeta_1^{c\delta+e\alpha+d\beta} = \sum_{c,\delta=0}^{q,\varepsilon} C(c,\delta)\zeta_1^{c\delta}\cdot\sum_{e,\alpha=0}^{s,\sigma} C(e,\alpha)\zeta_1^{e\alpha}\cdot\sum_{d,\beta=0}^{r,\tau} C(d,\beta)\zeta_1^{d\beta}$$

and (cf. the proof of Theorem 1.2)

$$\sum_{c,\delta=0}^{q,\varepsilon} C(c,\delta)\zeta_1^{c\delta}$$

has order $\geq e'q$ and $\geq e'\varepsilon$, hence order $\geq qi+\varepsilon i'$. Similarly for the others. In the second sum, let

$$C(d,e,\beta,\delta)n_{\delta,\beta,e,d}\zeta_1^{d\beta} = h(\delta,\beta,e,d).$$

Then the second sum is

$$\begin{aligned} &\pi^{pf}\sum_{d,e,\beta,\delta=0}^{r,s,\tau,\varepsilon} h(\delta,\beta,e,d)\cdot\sum_{c=0}^{q}\binom{q}{c}(-1)^{q-c}\zeta_1^{\delta c}\cdot\sum_{\alpha=0}^{\sigma}\binom{\sigma}{\alpha}(-1)^{\sigma-\alpha}\zeta_1^{e\alpha} \\ &= \pi^{pf}\sum_{d,e,\beta,\delta=0}^{r,s,\tau,\varepsilon} h(\delta,\beta,e,d)(\zeta_1^\delta-1)^q(\zeta_1^e-1)^\sigma, \end{aligned}$$

which has order $\geq pf+qe'+\sigma e'$. So we want

$$pf+qe'+\sigma e' \geq qi+rj+sk+\sigma k'+\tau j'+\varepsilon i'.$$

The worst case is when $q=\sigma=0, r=\tau=\varepsilon=s=p-1$, in which case we have

$$pf \geq (p-1)(i'+k+e'),$$

which holds since $f=(\frac{p-1}{p})(i'+k+e')$. □

Pairs of triangular R-Hopf orders satisfying the conditions of Theorem 3.7 are called *duality Hopf orders*.

Suppose a Hopf order $H \subseteq KC_{p^3}$ induces the short exact sequences

$$R \to A(i,j,u) \to H \to H(k) \to R$$

and

$$R \to A(k',j',z) \to H^* \to H(i') \to R.$$

Then H satisfies the "valuative condition for $n = 3$" [Un96, §4.0] if either $pk \le l$ or $pi' \le \hat{l}$, where $H(i,l) = \mathcal{L}(A(i,j,u))$ and $H(k',\hat{l}) = \mathcal{L}(A(k',j',z))$. If H satisfies this condition, then at least one of the short exact sequences above can be written as the Baer product of a generically trivial extension and a distinguished extension of Hopf orders. Hence the structure of H can be characterized. This generalizes Greither's method of [Gr92] for Hopf orders of rank p^2.

Recall that the maximal Larson order in $A(i,j,u)$ is $H(i,l)$, where

$$l = \begin{cases} j & \text{if } \operatorname{ord}(u-1) \ge i' + j, \\ i - e' + \operatorname{ord}(u-1) & \text{otherwise} \end{cases}$$

and the maximal Larson order in $A(k',j',z)$ is $H(k',\hat{l})$, where

$$\hat{l} = \begin{cases} j' & \text{if } \operatorname{ord}(z-1) \ge k + j', \\ k' - e' + \operatorname{ord}(z-1) & \text{otherwise.} \end{cases}$$

Theorem 3.8. *A duality Hopf order $A(i,j,k,u,v,w)$ satisfies the valuative condition.*

Proof. Since $e' > \operatorname{ord}(\hat{u}-1)$, and $e' > \operatorname{ord}(\hat{z}-1)$, then from (xi),

$$e' + \operatorname{ord}(\hat{z}-1) > e' + \frac{p-1}{p}(i' + k + e'),$$

hence

$$\operatorname{ord}(\hat{z}-1) > \frac{e'}{p},$$

and likewise, $\operatorname{ord}(\hat{u}-1) > e'/p$. Thus $\operatorname{ord}(u-1) = \operatorname{ord}(z-1) = e'/p$, which gives $pi' \le j'$ and $pk \le j$ by (v) and (vi).

By (xi) and Proposition 2.3, one has

$$\operatorname{ord}(G(\hat{u},\hat{z})-1) \ge \frac{p-1}{p}(i' + k + e') > \frac{e'}{p^2}.$$

Now if $i' + pk > e'/p$, then by (ii) $\operatorname{ord}(v^p\zeta_2 - 1) > e'/p$, thus since $vx\zeta_3 G(\hat{u},\hat{z}) = 1$, $\operatorname{ord}(x^p - 1) > e'/p$. So $e'/p \ge k + pi'$ by (viii), and the valuation condition $pi' \le \hat{l}$ holds.

If $e'/p \ge i' + pk$, then the valuation condition $pk \le l$ holds. □

Proposition 3.9. *Let $A(i,j,k,u,v,w)$ be duality. Then either $A(i,j,u)$ or $A(k',j',z)$ is dual Larson.*

Proof. If $\operatorname{ord}(\hat{u}-1) \geq i'+j$, then $A(i,j,u)$ is dual Larson, so suppose $i'+j > \operatorname{ord}(\hat{u}-1)$. Then by (xi),

$$\begin{aligned} i'+j+\operatorname{ord}(\hat{z}-1) &> e' + \frac{p-1}{p}(i'+k+e'), \\ i'+\operatorname{ord}(\hat{z}-1) &> j' + \frac{(p-1)i'}{p} + \frac{(p-1)k}{p} + \frac{e}{p}, \\ \operatorname{ord}(\hat{z}-1) &> j' + \frac{e-i'}{p} + \frac{(p-1)k}{p}, \\ \operatorname{ord}(\hat{z}-1) &> j' + \frac{i+(p-1)k}{p}, \\ \operatorname{ord}(\hat{z}-1) &> j'+k, \end{aligned}$$

since $i \geq k$. Thus $A(k',j',z)$ is dual Larson. □

In view of the above proposition and Theorem 3.8, it is natural to compare duality Hopf orders to the cohomological Hopf orders of Theorem 1.7. There are duality Hopf orders which are not cohomological, as the following example shows.

Example 3.10. Let $p=3, e'=306, e'/p=102, i=272, j=204, k=6$, so that $i'=34, j'=102, k'=300$. Let

- $\operatorname{ord}(\hat{u}-1)=237$, then
- $\operatorname{ord}(u-1)=102$; let
- $\operatorname{ord}(\hat{z}-1)=305$, then
- $\operatorname{ord}(z-1)=102$ and
- $\operatorname{ord}(G(\hat{u},\hat{z})-1)=237+305-306=236$. Choose x with
- $\operatorname{ord}(x-1)=34$ and
- $\operatorname{ord}(x^3\zeta_2-1)\geq 111$. Define v by $G(\hat{u},\hat{z})vx\zeta_3=1$, then
- $\operatorname{ord}(v-1)=37$ and
- $\operatorname{ord}(v^3\zeta_2-1)=102$.

Then one verifies that all of the valuation inequalities hold, to yield a pair of dual Hopf orders, as follows:

(i) $237=\operatorname{ord}(\hat{u}-1)\geq 216 \geq i'/3+j$;
(ii) $102=\operatorname{ord}(v^3\zeta_2-1) > i'+3k=52$;
(iii) $237=\operatorname{ord}(\hat{u}-1)\geq i'=34$;
(iv) $543=\operatorname{ord}(\hat{u}-1)+\operatorname{ord}(z^3-1)\geq 3k+i'+e'=358$;
(v) $102=\operatorname{ord}(z-1)\geq j'/3+k=40$;
(vi) $102=\operatorname{ord}(u-1)\geq i'+j/3=102$;
(vii) $305=\operatorname{ord}(\hat{z}-1)\geq j'+k/3=104$;
(viii) $\operatorname{ord}(x^p\zeta_2-1)\geq 111 > 108=k+3i'$;
(ix) $305=\operatorname{ord}(\hat{z}-1)\geq k=6$;
(x) $611=\operatorname{ord}(\hat{z}-1)+\operatorname{ord}(u^p-1)\geq 3i'+k+e'=414$;
(xi) $542=\operatorname{ord}(\hat{z}-1)+\operatorname{ord}(\hat{u}-1)\geq 537 \geq e'+(\frac{2}{3})(k+i'+e')$.

Now $A(i,j,u)=A(272,204,u)$ is not dual Larson, but $A(k',j',z)=A(300,102,z)$ is dual Larson, but not Larson. We have $\mathcal{L}(A(300,102,z))=H(300,96)$. However, $3i' \not\leq 96$ as required for $A(k',j',i',z,x,y)$ to be cohomological.

Moreover, no cohomological Hopf order with $e'/p > \operatorname{ord}(w-1) = \operatorname{ord}(\hat{z}-1)$ can be duality, for by (xi) and (i) of Theorem 3.7, $\operatorname{ord}(\hat{z}-1)$ must satisfy

$$e' + \operatorname{ord}(\hat{z}-1) \geq \operatorname{ord}(\hat{u}-1) + \operatorname{ord}(\hat{z}-1) \geq e' + (\frac{p-1}{p})(e'+i'+k).$$

Remark 3.11. Now that we have discussed triangular Hopf orders in some detail, a natural question arises: Is every Hopf order in KC_{p^3} triangular? Intuitively, the answer would seem to be "no". Suppose H is a rank p^3 Hopf order that is an extension of a rank p^2 Hopf order by $H(i)$. The classes of examples we have constructed require that the parameter i be close to e'. For example, if H is a duality Hopf order, then inequalities (iii) and (vi) of Theorem 3.7 are

$$\text{(iii)}\ \ \operatorname{ord}(\hat{u}-1) \geq i',$$
$$\text{(vi)}\ \ \operatorname{ord}(u-1) \geq i' + j/p.$$

Since $\hat{u} = (u\zeta_2)^{-1}$, it follows from (iii) and (vi) that

$$e'/p \geq i'$$

and hence

$$i \geq \left(\frac{p-1}{p}\right) e'.$$

Similarly, if H is a ILD Hopf order, then $i' \leq e'/p$. Thus a rank p^3 Hopf order that is an extension of a rank p^2 Hopf order by $H(i)$, where i is sufficiently smaller than e', cannot be duality or ILD.

In fact, we essentially showed in [CU03] that there are Hopf orders arising from formal groups with i sufficiently smaller than e' that cannot be triangular. In the next section we review this result, and investigate the relationship between "formal group" Hopf orders and triangular Hopf orders in more detail.

4. Formal group Hopf orders

In [CU03, Theorem 2.1] the authors give a general construction of Hopf orders in KC_{p^n} as the representing algebras of kernels of isogenies $f: \mathcal{F} \to \mathcal{G}$ of degree 2 dimension n polynomial formal groups. These are the so-called *formal group Hopf orders*. We obtained the following theorem:

Theorem 4.1 ([CU03, Theorem 2.1])**.** *Suppose Θ is an $n \times n$ lower triangular matrix with entries in R for which $\det(\Theta) \neq 0$ and $\operatorname{ord}(\theta_{r,r}) > 0$ for all r. Suppose, for all ℓ, that $\operatorname{ord}(\theta_{\ell,i}) < \operatorname{ord}(\theta_{\ell,\ell})$ for all $i < \ell$ such that $\theta_{\ell,i} \neq 0$, and suppose also that there exists numbers q and d so that $\operatorname{ord}(\theta_{\ell,i}) \geq (1-q)\operatorname{ord}(\theta_{\ell,\ell})$ and $\operatorname{ord}(\theta_{\ell,\ell}) \geq d \operatorname{ord}(\theta_{\ell+1,\ell+1})$, where*

$$0 < q < \frac{p-1}{2p-1},$$
$$\operatorname{ord}(\theta_{1,1}) < \left(\frac{p-1}{p}\right)\left(\frac{d-1}{d-1+q}\right) e'$$

and

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

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

Remark 4.2. The structure of H_Θ can be determined as follows. Let $U = (u_{i,j})$ denote the lower triangular matrix which is the inverse of Θ. Then, following [CS98, p. 71],

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

where

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

and $\langle g \rangle = C_{p^n}$.

In this section we relate formal group Hopf orders when $n = 3$ to the classes of triangular Hopf orders of the previous sections.

We begin by recalling a result from [CU03]. Suppose $q \in \mathbb{Q}$ satisfies

$$0 < q < \frac{p-1}{2p-1}.$$

Put

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

Let i and j be integers with $i > dj$ and

$$i \leq \left(\frac{p-1}{p}\right)\left(\frac{d-1}{d-1+q}\right)e'.$$

Let s and k be integers with $j > dk$, $s < k$, and $s = (1-q)k$, that is, $q = 1 - \frac{s}{k}$. Set

$$\Theta = \begin{pmatrix} \pi^i & 0 & 0 \\ 0 & \pi^j & 0 \\ 0 & \pi^s & \pi^k \end{pmatrix}.$$

Then by Theorem 4.1, Θ yields an R-Hopf order H_Θ in KC_{p^3} of the form

$$H_\Theta = R\left[\frac{g^{p^2}-1}{\pi^i}, \frac{g^p - 1}{\pi^j}, \frac{-\pi^s(g^p-1)}{\pi^{j+k}} + \frac{g-1}{\pi^k}\right].$$

In [CU03, Theorem 4.2] we proved that if $i < (1 - \frac{1}{p} - \frac{1}{p^2})e'$, then H_Θ is not of the form

$$R\left[\frac{g^{p^2}-1}{\pi^i}, \frac{g^p-1}{\pi^j}, \frac{b_{x,y}g - 1}{\pi^k}\right].$$

A review of the proof of [CU03, Theorem 4.2] shows that with only obvious notational changes, that proof yields:

Theorem 4.3. *If*

$$i < \left(1 - \frac{1}{p} - \frac{1}{p^2}\right)e',$$

then the R-Hopf order H_Θ in KC_{p^3} defined above is not triangular.

We can also show that not every triangular Hopf order is formal group.

Theorem 4.4. *Suppose $p > 2$. Let $H = H(i, j, k, u, v, w)$ be an ILD Hopf order with $j' + (k/p) \leq \mathrm{ord}(w - 1) < j' + (k/2)$. Then H cannot represent the kernel of any isogeny of formal groups $f : \mathcal{F} \to \mathcal{G}$.*

Proof. H induces the short exact sequence

$$R \to H(i) \to H \to H(j, k, w) \to R,$$

where $H(j, k, w)$ is a Greither order in KC_{p^2}. Suppose H represents the kernel of an isogeny $f : \mathcal{F} \to \mathcal{G}$. Then the coalgebra structure of H is induced by the 3-dimensional polynomial formal group $\mathcal{F}$. It follows that the coalgebra structure of the Greither order $H(j, k, w)$ is induced by a 2-dimensional polynomial formal group $\mathcal{F}'$. But this contradicts [CU03, Theorem 3.0] since $\mathrm{ord}(1 - w) < j' + (k/2)$. □

Confirming a statement in Remark 3.11, we have

Proposition 4.5. *Suppose H_Θ is a formal group Hopf order of rank p^3, where $\mathrm{ord}(\theta_{1,1})$ satisfies the inequality*

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

of Theorem 4.1. Then H_Θ is not an ILD Hopf order.

The proof is trivial: any ILD Hopf order satisfies $e'/p \geq i'$, hence $i \geq (\frac{p-1}{p})e'$.

Triangular and formal group Hopf orders are not mutually exclusive, however. Certainly any Larson order in KC_{p^3} is both formal group and triangular. To see more precisely how formal group Hopf orders and their duals relate to triangular Hopf orders, we need to look more carefully at formal group Hopf orders when $n = 3$. Theorem 4.1 gives sufficient conditions to construct Hopf orders for any n, but when $n = 3$, it is not sharp. Here is a more precise result when $n = 3$, one that allows i to be close to e'.

Theorem 4.6. *Let*

$$\Theta = \begin{pmatrix} \pi^i & 0 & 0 \\ b\pi^r & \pi^j & 0 \\ c\pi^s & d\pi^t & \pi^k \end{pmatrix}$$

with b, c, d units of R, where $r < j$ and $s, t < k$, . Then the R-algebra H_Θ is a Hopf order in KC_{p^3} if the following inequalities hold:

$$\begin{aligned} e' > i > pj, \\ 2r \geq j > r > pk, \\ 2t \geq k > t, \\ 2s \geq k > s, \\ (p-1)i' = (p-1)(e'-i) > p(k-s), \\ (p-1)i' = (p-1)(e'-i) > p(j-r) + p(k-t), \\ i - pj > p(k-t), \\ 2r - j \geq k - t. \end{aligned}$$

Proof. We begin with a brief review of the construction of formal group Hopf orders of [CU03] adapted to the $n = 3$ case. Let $\overline{x} = (x_1, x_2, x_3)^T$, $\overline{y} = (y_1, y_2, y_3)^T$, and let $\mathbb{G}_m^3$ denote the 3-dimensional multiplicative formal group. Let Θ be a 3×3

lower triangular matrix with entries θ_{ij}. Under certain conditions on the entries of Θ, there exist 3-dimensional formal groups $\mathcal{F}$ and $\mathcal{F}^{(p)}$ defined by

$$\mathcal{F}(\overline{x},\overline{y}) = \Theta^{-1}\mathbb{G}_m^3(\Theta\overline{x},\Theta\overline{y}),$$
$$\mathcal{F}^{(p)}(\overline{x},\overline{y}) = (\Theta^{(p)})^{-1}\mathbb{G}_m^3(\Theta^{(p)}\overline{x},\Theta^{(p)}\overline{y}),$$

respectively, where $\Theta^{(p)}$ denotes the 3×3 matrix whose ijth entry is θ_{ij}^p. Let $[*]:\ \mathbb{G}_m^3 \to \mathbb{G}_m^3$ denote the homomorphism of formal groups defined by

$$[*](\overline{x}) = ((1+x_1)^p - 1, (1+x_1)^{-1}(1+x_2)^p - 1, (1+x_2)^{-1}(1+x_3)^p - 1)^T.$$

Then one can impose additional restrictions on Θ so that the map

$$f(\overline{x}) = (\Theta^{(p)})^{-1}[*](\Theta\overline{x})$$

is an isogeny of formal groups $f:\ \mathcal{F} \to \mathcal{F}^{(p)}$. The representing algebra of the kernel of f is a Hopf order in KC_{p^3} of the form H_Θ.

To construct H_Θ we first find conditions for the formal group $\mathcal{F}$ to be defined over R. Since $\mathcal{F}(\overline{x},\overline{y}) = \Theta^{-1}\mathbb{G}_m^3(\Theta\overline{x}),\Theta\overline{y})$, it is routine to verify that

$$\begin{aligned}
\mathcal{F}_1 &= x_1 + y_1 + \pi^i x_1 y_1,\\
\mathcal{F}_2 &= x_2 + y_2 + \left(\frac{-b\pi^{r+2i}}{\pi^{i+j}}\right)x_1y_1 + \left(\frac{b^2\pi^{2r}}{\pi^j}\right)x_1y_1 + b\pi^r(x_1y_2 + x_2y_1) + \pi^j x_2y_2,\\
\mathcal{F}_3 &= x_3 + y_3 + \left(\frac{\pi^{2i}(bd\pi^{r+t} - c\pi^{s+j})}{\pi^{i+j+k}} - \frac{d\pi^t b^2\pi^{2r}}{\pi^{j+k}} + \frac{c^2\pi^{2s}}{\pi^k}\right)x_1y_1\\
&\quad + \left(\frac{-bd\pi^t\pi^{r+j}}{\pi^{j+k}} + \frac{cd\pi^{s+t}}{\pi^k}\right)(x_1y_2 + x_2y_1) + \left(\frac{c\pi^{s+k}}{\pi^k}\right)(x_1y_3 + x_3y_1)\\
&\quad + \left(\frac{-d\pi^t\pi^{2j}}{\pi^{j+k}} + \frac{d^2\pi^{2t}}{\pi^k}\right)x_2y_2 + \left(\frac{d\pi^{t+k}}{\pi^k}\right)(x_2y_3 + x_3y_2) + \pi^k x_3y_3.
\end{aligned}$$

So $\mathcal{F}$ is defined over R if each of the above coefficients is in R, which is the case if the following inequalities hold:

$$\begin{aligned}
r + i &\geq j,\\
2r &\geq j,\\
s + i &\geq k,\\
i + r + t &\geq j + k,\\
t + 2r &\geq j + k,\\
t + r &\geq k,\\
t + j &\geq k,\\
2t &\geq k,\\
s + t &\geq k,\\
2s &\geq k.
\end{aligned}$$

We also need $\mathcal{F}^{(p)}(\overline{x},\overline{y}) = (\Theta^{(p)})^{-1}\mathbb{G}_m^3(\Theta^{(p)}\overline{x},\Theta^{(p)}\overline{y})$ to be defined over R, but the inequalities become the same. Now we seek conditions on Θ so that $f(\overline{x})$ is

defined over R, where

$$f(\overline{x}) = (\Theta^{(p)})^{-1}[*](\Theta\overline{x}) = (\Theta^{(p)})^{-1}\begin{pmatrix}\eta_1\\ \eta_2\\ \eta_3\end{pmatrix},$$

where

$$\eta_1 = (1+\theta_{1,1}x_1)^p - 1,$$
$$\eta_2 = \frac{(1+\theta_{2,1}x_1+\theta_{2,2}x_2)^p - (1+\theta_{1,1}x_1)}{(1+\theta_{1,1}x_1)},$$
$$\eta_3 = \frac{(1+\theta_{3,1}x_1+\theta_{3,2}x_2+\theta_{3,3}x_3)^p - (1+\theta_{2,1}x_1+\theta_{2,2}x_2)}{1+\theta_{2,1}x_1+\theta_{2,2}x_2}.$$

Assuming that $\operatorname{ord}(\theta_{i,j}) < e'$ for all i,j such that $\theta_{i,j} \neq 0$, we have $[*](\Theta\overline{x}) =$

$$\begin{pmatrix}\theta_{1,1}^p x_1^p + p\theta_{1,1}z_1'\\ (\theta_{2,1}^p x_1^p + \theta_{2,2}^p x_2^p + p\theta_{2,1}z_2' - \theta_{1,1}x_1)(1-\theta_{1,1}z_3')\\ (\theta_{3,1}^p x_1^p + \theta_{3,2}^p x_2^p + \theta_{3,3}^p x_3^p + p\theta_{3,1}z_4' + p\theta_{3,2}z_5' - \theta_{2,1}x_1 - \theta_{2,2}x_2)(1+\theta_{2,1}\pi^r z_6')\end{pmatrix}$$

with z_i' in $R[[\overline{x}]]$.

Inserting the entries of Θ, we find that $f(x) = \overline{x}^{(p)} + w$, where $\overline{x}^{(p)} = (x_1^p, x_2^p, x_3^p)^T$ and $w = (w_1, w_2, w_3)^T$, where

$$w_1 = \frac{p\pi^i}{\pi^{pi}}z_1,$$
$$w_2 = \frac{\pi^{pr}p\pi^i}{\pi^{pi+pj}}z_2 + \frac{p\pi^r}{\pi^{pj}}z_3 + \frac{\pi^i}{\pi^{pj}}z_4,$$
$$w_3 = \frac{p\pi^{i+ps}}{\pi^{pi+pk}}z_5 + \frac{p\pi^{i+pr+pt}}{\pi^{pi+pj+pk}}z_6 + \frac{p\pi^{pt+r}}{\pi^{pj+pk}}z_7 + \frac{\pi^{pt+i}}{\pi^{pj+pk}}z_8 + \frac{p\pi^s}{\pi^{pk}}z_9 + \frac{p\pi^t}{\pi^{pk}}z_{10} + \frac{\pi^r}{\pi^{pk}}z_{11}$$

with $z_1, \ldots, z_{11}$ in $R[[\overline{x}]]$. Thus for $f(\overline{x})$ to be defined over R with

$$f(\overline{x}) \equiv \overline{x}^{(p)} \pmod{\pi R[[\overline{x}]]}$$

it suffices that the following inequalities hold:

$$e+i > pi,$$
$$e+pr+i > pi+pj,$$
$$e+r > pj,$$
$$i > pj,$$
$$e+i+ps > pi+pk,$$
$$e+i+pr+pt > pi+pj+pk,$$
$$e+pt+r > pj+pk,$$
$$pt+i > pj+pk,$$
$$e+s > pk,$$
$$e+t > pk,$$
$$r > pk.$$

Collecting the two sets of inequalities for $\mathcal{F}$ and f yields the theorem. □

These inequalities immediately yield:

Corollary 4.7. *If $H = H_\Theta$ is a formal group Hopf order arising from Theorem 4.1 or Theorem 4.6 and $p > 2$ or $k > 0$ or $i < e'$ or $j < i/p$ or $j' < k'/p$, then H^* cannot be a formal group Hopf order.*

Proof. Considering the hypotheses of each theorem, the valuation parameters i, j and k of H satisfy $i \geq pj$ and $j \geq pk$. The valuation parameters of H^* are then k', j' and i', and for H^* to be a formal group Hopf order they would have to satisfy $k' \geq pj'$ and $j' \geq pi'$. But then $j \leq i/p \leq e'/p$ and $j' \leq k'/p \leq e'/p$, hence $e' \leq 2e'/p$, which means that $p = 2$ and all the inequalities in the statement of the corollary are equalities. □

To treat duals of formal group Hopf orders arising from Theorem 4.6, we will use the following general duality result.

Theorem 4.8. *Let K contain a primitive p^nth root of unity ζ_n, and let $G = \langle g \rangle$ be cyclic of order p^n with character group $\hat{G} = \langle \gamma \rangle$. Let $H \subset KG$ be a Hopf order and let $H_1 = H \cap K\langle g^{p^{n-1}} \rangle = H(i)$ with $0 \leq i < e'$. Let $\overline{H}$ = image of H modulo $\langle g^{p^{n-1}} \rangle$. Let $A = \overline{H}^* \subset K\langle \gamma^p \rangle$. Let*

$$J = A\left[\frac{u\gamma - 1}{\pi^{i'}}\right]$$

with $u \in K\langle \gamma^p \rangle$. If $\langle J, H \rangle_n \subset R$, then $J = H^*$ is a Hopf order in $K\hat{G}$.

Proof. First, we show that $\alpha = \frac{u\gamma - 1}{\pi^{i'}}$ satisfies a monic polynomial of degree p with coefficients in A.

We have

$$\gamma^p u^p = (1 + \alpha\pi^{i'})^p \in K[\langle \gamma^p \rangle],$$

and so since $e = (p-1)e' \geq (p-1)i'$,

$$\alpha^p + \sum_{r=1}^{p-1} \binom{p}{r} \alpha^r \pi^{(r-p)i'} = \frac{u^p\gamma^p - 1}{\pi^{pi'}}$$

is in $H^* \cap K\langle \gamma^p \rangle = A$. Thus u is a unit of A.

Now if A has an R-basis $\{a_\nu\}$, $\nu = 1, \ldots, p^{n-1}$, then J has an R-basis $\{a_\nu \alpha^k\}$ with $\nu = 1, \ldots, p^{n-1}$, $k = 0, \ldots, p-1$, a basis with which we can compute the discriminant of J. The discriminant of H^* may be obtained by dualizing the exact sequence of Hopf orders,

$$R \to H(i) = H_1 \to H \to \overline{H} \to R.$$

We obtain

$$R \to A \to H^* \to H_1^* \to R$$

from which we have (from [Gr92]; cf. [C00, (22.18)])

$$disc(H^*) = disc(A)^p disc(H_1^*)^{p^{n-1}} = disc(A)^p \pi^{p^{n-1}p(p-1)i} R,$$

since $H_1^* = H(i')$ and $disc(H(i')) = \pi^{p(p-1)i}R$ by [C00, (21.1)].

Now $J_0 = A[u\gamma - 1] = A[\gamma]$ is a Hopf order in $K\hat{G}$, and we can compute the discriminant of $A[\gamma]$ using the exact sequence:

$$R \to A \to J_0 \to H(0) \to R,$$

namely,

$$disc(J_0) = disc(A)^p disc(H(0))^{p^{n-1}} = disc(A)^p \pi^{p^{n-1}p(p-1)e'} R.$$

The matrix that multiplies the basis $\{a_\nu \alpha^k\}$ of J to the basis $\{a_\nu (u\gamma - 1)^k\}$ of J_0 is the matrix

$$M = diag(1, \dots, 1, \pi^{i'}, \dots, \pi^{i'}, \dots, \pi^{(p-1)i'}, \dots, \pi^{(p-1)i'}),$$

whose determinant is $\pi^{i'(p^{n-1}p(p-1))/2}$. So

$$disc(J_0) = det(M)^2 disc(J) = \pi^{p^{n-1}p(p-1)i'} disc(J),$$

and hence

$$\begin{aligned} disc(J) &= disc(J_0)\pi^{-p^{n-1}p(p-1)i'} R \\ &= disc(A)^p \pi^{p^{n-1}p(p-1)e' - p^{n-1}p(p-1)i'} R \\ &= disc(A)^p \pi^{p^{n-1}p(p-1)i} R = disc(H^*). \end{aligned}$$

Since $J \subset H^*$ and have equal discriminants, $J = H^*$. □

We now show that the dual of a formal group Hopf order of rank p^3 is triangular. Let

$$\Theta = \begin{pmatrix} \pi^i & 0 & 0 \\ b\pi^r & \pi^j & 0 \\ c\pi^s & d\pi^t & \pi^k \end{pmatrix}$$

with b, c, d units of R, satisfying Theorem 4.6, and let $U = (u_{i,j})$ be the inverse of Θ. Then $H_\Theta = R[z_1, z_2, z_3]$, where

$$\begin{aligned} z_1 &= u_{1,1}(g^{p^2} - 1), \\ z_2 &= u_{2,1}(g^{p^2} - 1) + u_{2,2}(g^p - 1), \\ z_3 &= u_{3,1}(g^{p^2} - 1) + u_{3,2}(g^p - 1) + u_{3,3}(g - 1). \end{aligned}$$

Let

$$J = R\left[\frac{\gamma^{p^2} - 1}{\pi^{k'}}, \frac{a_z \gamma^p - 1}{\pi^{j'}}, \frac{a_x b_y \gamma - 1}{\pi^{i'}}\right]$$

with z satisfying

$$u_{3,2}(\zeta_1 - 1) + u_{3,3}(\zeta_2 z - 1) = 0,$$

with y satisfying

$$u_{2,1}(\zeta_1 - 1) + u_{2,2}(\zeta_2 y - 1) = 0$$

and with x satisfying

$$u_{3,1}(\zeta_1 - 1) + u_{3,2}(\zeta_2 y - 1) + u_{3,3}(\zeta_3 x - 1) = 0.$$

Then one sees easily that

$$\begin{aligned} z &= \zeta_2^{-1}(1 + \pi^{t-j} d(\zeta_1 - 1)), \\ y &= \zeta_2^{-1}(1 + \pi^{r-i} b(\zeta_1 - 1)) \end{aligned}$$

and

$$x = \zeta_3^{-1}(1 + \pi^{s-i} c(\zeta_1 - 1)).$$

Theorem 4.9. *Suppose Θ is as above so that $\mathcal{F}_\Theta$ and the isogeny f_Θ are defined over R. Then the dual of H_Θ is triangular.*

Proof. We show that $H_\Theta^* = J$, defined above. Using Theorem 4.8 it suffices to show that

$$\langle J, H_\Theta \rangle \subset R.$$

We know that

$$J_0 = R\left[\frac{\gamma^{p^2}-1}{\pi^{k'}}, \frac{a_z\gamma^p - 1}{\pi^{j'}}\right]$$

is the dual of H_{Θ_2}, the image of H_Θ under the map sending g^{p^2} to 1, where

$$\Theta_2 = \begin{pmatrix} \pi^j & 0 \\ d\pi^t & \pi^k \end{pmatrix}.$$

So since H_Θ is a Hopf order and its dual contains J_0, it suffices to show that $\frac{a_x b_y \gamma - 1}{\pi^{i'}}$ is in H_Θ^*. So we need to show that for all $0 \le l, m, n \le p-1$,

$$\langle a_x b_y \gamma - 1, z_1^l z_2^m z_3^n \rangle \in \pi^{i'} R.$$

Since

$$\langle 1, z_1^l z_2^m z_3^n \rangle = 0$$

for $l + m + n > 0$ and

$$\langle a_x b_y \gamma - 1, 1 \rangle = 0,$$

it suffices to show that

$$\langle a_x b_y \gamma, z_1^l z_2^m z_3^n \rangle \in \pi^{i'} R$$

for $l + m + n > 0$. Now we have

$$\langle a_x b_y \gamma, g^{p^2 r + ps + t} \rangle = \zeta_1^r (y\zeta_2)^s (x\zeta_3)^t$$

for $0 \le s, t \le p-1$ and any $r \ge 0$. So for $0 < m + n \le p-1$, we have

$$\begin{aligned}\langle a_x b_y \gamma, z_1^l z_2^m z_3^n \rangle &= (u_{1,1}(\zeta_1 - 1))^l (u_{2,1}(\zeta_1 - 1) + u_{2,2}(y\zeta_2 - 1))^m \\ &\quad \cdot (u_{3,1}(\zeta_1 - 1) + u_{3,2}(y\zeta_2 - 1) + u_{3,3}(x\zeta_3 - 1))^n \\ &= 0,\end{aligned}$$

by the way we defined x and y.

Since

$$u_{2,1}(\zeta_1 - 1) + u_{2,2}(y\zeta_2 - 1) = 0$$

we have

$$\begin{aligned} z_2 &= u_{2,1}(g^{p^2} - 1) + u_{2,2}(g^p - 1) \\ &= u_{2,1}(g^{p^2} - \zeta_1) + u_{2,2}(g^p - y\zeta_2)\end{aligned}$$

and since

$$u_{3,1}(\zeta_1 - 1) + u_{3,2}(y\zeta_2 - 1) + u_{3,3}(x\zeta_3 - 1) = 0$$

we have

$$\begin{aligned} z_3 &= u_{3,1}(g^{p^2} - 1) + u_{3,2}(g^p - 1) + u_{3,3}(g - 1) \\ &= u_{3,1}(g^{p^2} - \zeta_1) + u_{3,2}(g^p - y\zeta_2) + u_{3,3}(g - x\zeta_3).\end{aligned}$$

Set $b_1 = g^{p^2} - \zeta_1, b_2 = g^p - y\zeta_2, b_3 = g - x\zeta_3$. If we set $\lambda = \zeta_1 - 1$, then we have

$$z_1 = u_{1,1}(b_1 + \lambda),$$

and

$$z_1^l z_2^m z_3^n = u_{1,1}^l (b_1 + \lambda)^l (u_{2,1}b_1 + u_{2,2}b_2)^m (u_{3,1}b_1 + u_{3,2}b_2 + u_{3,3}b_3)^n$$

is an R-linear combination of terms of the form

$$B = u_{1,1}^{l}\lambda^{l_2}u_{2,1}^{m_1}u_{2,2}^{m_2}u_{3,1}^{n_1}u_{3,2}^{n_2}u_{3,3}^{n_3}b_1^{l_1+m_1+n_1}b_2^{m_2+n_2}b_3^{n_3}$$

with $l_1 + l_2 = l, m_1 + m_2 = m < p$, and $n_1 + n_2 + n_3 = n < p$.

Set

$$\phi = \langle a_x b_y \gamma, - \rangle : KG \to K.$$

Then ϕ maps RG to R and $\phi(B) = 0$ if $l_1 + m_1 + n_1 > 0$ or $n_3 > 0$. Thus $\phi(z_1^l z_2^m z_3^n)$ is a linear combination of terms of the form

$$u_{1,1}^{l}\lambda^{l}u_{2,2}^{m}u_{3,2}^{n}\phi(b_2^{m+n}).$$

Terms of this form equal 0 if $0 < m + n < p$. If $m + n = p + t$, then

$$\phi(b_2^{p+t}) = p\phi(\xi) + \phi((g^{p^2} - y^p\zeta_1)(g^p - \zeta_2 y)^t)$$

with ξ in RG. The second term in the right side equals 0 if $t > 0$, and $= \zeta_1(1 - y^p)$ if $m + n = p$. Thus, with $m + n = p + t$, $\phi(z_1^l z_2^m z_3^n)$ is a linear combination of terms of the form

$$(u_{1,1}\lambda)^l u_{2,2}^m u_{3,2}^n p\phi(\xi) + (u_{1,1}\lambda)^l u_{2,2}^m u_{3,2}^n(\zeta_1(1 - y^p))$$

with $\phi(\xi) \in R$ and the second term occurring only for $m + n = p$.

Note that

$$\begin{aligned}
\operatorname{ord}(u_{2,2}) &= -j,\\
\operatorname{ord}(u_{3,2}) &= t - j - k,\\
\operatorname{ord}(u_{1,1}) &= -i,\\
\operatorname{ord}(1 - y^p) &\geq min\{e', pi' + pr\}.
\end{aligned}$$

Thus

$$\operatorname{ord}((u_{1,1}\lambda)^l u_{2,2}^m u_{3,2}^n p) \geq i'$$

follows if

$$l(e' - i) - mj - n(t - j - k) + e > i'$$

and for that to hold (since $\operatorname{ord}(u_{1,1}\lambda) > 0$) it suffices that

$$e > i' + (p - 1)j + (p - 1)(j + (k - t)).$$

But $i > pj + p(k - t)$ from Theorem 4.6, so

$$i' + (p - 1)j + \left(\frac{p - 1}{p}\right) i \geq i' + (p - 1)j + (p - 1)(j + (k - t)).$$

Now $\left(\frac{2(p-1)}{p}\right) i + i' > i' + (p - 1)j + \left(\frac{p-1}{p}\right) i$ since $i > pj$, and $e \geq \left(\frac{2(p-1)}{p}\right) i + i'$ since $e' \geq i$, thus the required inequality holds.

Also, for $m + n = p$,

$$\operatorname{ord}((u_{1,1}\lambda)^l u_{2,2}^m u_{3,2}^n \zeta_1(1 - y^p)) \geq i'$$

if

$$\begin{aligned}
min\{e', pi' + pr\} + m(-j) + n(-j - k + t)&\\
\geq min\{e', pi' + pr\} - pj + (p - 1)(t - k) \geq i'&
\end{aligned}$$

or

$$min\{e', pi' + pr\} + i - pj - (p - 1)(k - t) \geq e'.$$

But from Theorem 4.6, we have

$$i - pj - (p - 1)(k - t) > 0$$

so the desired inequality follows if $min\{e', pi' + pr\} \geq e'$. To show

$$pi' + pr - pj - (p-1)(k-t) \geq i'$$

it suffices to show that

$$(p-1)i' \geq p(j-r) + (p-1)(k-t)$$

which follows from the inequality from Theorem 4.6:

$$(p-1)i' \geq p(j-r) + p(k-t).$$

This completes the proof. □

We seek conditions so that H_Θ itself is triangular.

Theorem 4.10. *Suppose Θ is as above so that $\mathcal{F}_\Theta$ and the isogeny f_Θ are defined over R. Then $J = H_\Theta^*$ is ILD if $e'/p > i' + r$ and $e'/p \geq k + pi'$.*

Proof. From Theorem 4.9 we have the triangular Hopf order

$$H_\Theta^* = J = R\left[\frac{\gamma^{p^2}-1}{\pi^{k'}}, \frac{a_z\gamma^p - 1}{\pi^{j'}}, \frac{a_x b_y \gamma - 1}{\pi^{i'}}\right]$$

with

$$z = \zeta_2^{-1}(1 + \pi^{t-j} d(\zeta_1 - 1)),$$
$$y = \zeta_2^{-1}(1 + \pi^{r-i} b(\zeta_1 - 1))$$

and

$$x = \zeta_3^{-1}(1 + \pi^{s-i} c(\zeta_1 - 1)).$$

Note $e'/p \geq k$ by Theorem 4.6, so the Hopf order $\mathcal{LD}(A(k', j', z))$ exists. Since $\mathrm{ord}(\hat{z} - 1) = t + j' < k + j'$,

$$\mathcal{LD}(A(k', j', z)) = H(\varrho', k)^* = H(k', \varrho, \zeta_2^{-1}),$$

where ϱ satisfies $\mathrm{ord}(\hat{z} - 1) = k + \varrho$. Thus $\varrho' = k + j - t$.

Let l satisfy

$$\begin{cases} l = \varrho \text{ if } e'/p \geq k + \varrho, \\ e'/p = k + l \text{ if } e'/p < k + \varrho. \end{cases}$$

We need $pi' \leq l$. If $e'/p < k + \varrho$, this follows from the assumption $e'/p \geq k + pi'$. But by a condition of Theorem 4.6, we have $(p-1)e' > p(j-t)$, which yields $k + \varrho > e'/p$, and so $pi' \leq l$. Thus J is ILD if the inequalities (A)–(D) hold, where

(A) $$\mathrm{ord}(1 - x^p) \geq k + pi',$$

(B) $$\mathrm{ord}(1 - y) \geq (k + j - t)/p + i',$$

(C) $$\mathrm{ord}(1 - y) \geq k + j - t + (i'/p),$$

(D) $$\mathrm{ord}(1 - x^p y^{-1}) \geq pk + i'.$$

(A) We have

$$\mathrm{ord}(1 - x^p) \geq min\{e'/p, pi' + ps, e + i' + s\}$$

thus (A) holds given that $e'/p \geq pi' + k$, $ps \geq k$, and $e + i' + s \geq pi' + k$.

(B) Since $e'/p > i' + r$, $\mathrm{ord}(1 - y) = i' + r$. Now

$$i' + r \geq (k + j - t)/p + i'$$

follows from $t + 2r \geq j + k$, a condition of Theorem 4.6.

(C) The condition of Theorem 4.6: $(p-1)i' \geq p(k-t)+p(j-r)$ implies (C).
(D) We have

$$\operatorname{ord}(1-y^{-1}x^p) \geq min\{e+i'+s, i'+r, pi'+ps\},$$

which implies (D) by Theorem 4.6. □

We conclude this section by finding sufficient conditions on a formal group Hopf order H to be triangular. Since H^* is triangular by Theorem 4.9, if we find conditions on H^* to be duality, then H will be triangular.

Proposition 4.11. *Let $J = A(k', j', i', z, x, y)$ be the dual of a formal group Hopf order H_Θ with Θ as in Theorem 4.6. If $\operatorname{ord}(\hat{y}-1) = i'+r = e'/p$ and $\operatorname{ord}(y-1)$ satisfies $e' > \operatorname{ord}(1-y)$ and*

$$\operatorname{ord}(\hat{z}-1)+\operatorname{ord}(y-1) = t+j'+\operatorname{ord}(y-1) \geq e'+\left(\frac{p-1}{p}\right)(e'+i'+k),$$

then H_Θ is triangular.

Proof. We have

$$\begin{aligned}\operatorname{ord}(\hat{z}-1) &= t+j',\\ \operatorname{ord}(\hat{y}-1) &= r+i',\\ \operatorname{ord}(x\zeta_3-1) &= s+i',\end{aligned}$$

where i, j, k, r, s, t satisfy the inequalities of Theorem 4.6. Following Theorem 3.7, $H = A(i, j, k, u, v, w)$ is free of rank p over $A(i, j, u)$ if (Proposition 3.5)

(i) $\operatorname{ord}(u-1) \geq i'+j/p$,
(ii) $\operatorname{ord}(\hat{u}-1) \geq i'/p+j$,
(iii) $\operatorname{ord}(v^p\zeta_2-1) \geq i'+pk$,
(iv) $\operatorname{ord}(\hat{u}-1) \geq i'$,
(v) $\operatorname{ord}(w\zeta_2-1) \geq j'/p+k$,
(vi) $\operatorname{ord}(\hat{u}-1)+\operatorname{ord}(w^p\zeta_1-1) \geq e'+i'+pk$,

and $H = J^*$ if $w = \hat{z}, y = \hat{u}, vx\zeta_3 G(\hat{u}, \hat{z}) = 1$ and

(xi) $\operatorname{ord}(\hat{z}-1)+\operatorname{ord}(\hat{u}-1) \geq e'+(\frac{p-1}{p})(e'+i'+k)$.

To begin with condition (xi), $\operatorname{ord}(\hat{z}-1) = j'+t$, so $\operatorname{ord}(\hat{u}-1) = \operatorname{ord}(y-1)$ must satisfy

$$\operatorname{ord}(\hat{u}-1) = \operatorname{ord}(y-1) \geq e'+\left(\frac{p-1}{p}\right)(e'+i'+k)-(j'+t).$$

Now $\operatorname{ord}(\hat{y}-1) = i'+r$. From Remark 1.4, if $\operatorname{ord}(\hat{y}-1) \neq e'/p$, then $\operatorname{ord}(y-1) \leq e'/p$; but

$$e'/p \geq e'+\left(\frac{p-1}{p}\right)(e'+i'+k)-(j'+t)$$

is impossible for $p \geq 3$, for

$$j'+t+e'/p < e'+e'/p+e'/p^2 < e'+\left(\frac{p-1}{p}\right)e' < e'+\left(\frac{p-1}{p}\right)(e'+i'+k).$$

Thus we must have $\operatorname{ord}(\hat{y}-1) = i'+r = e'/p$ and $\operatorname{ord}(y-1)$ so large (but still $< e'$) that (xi) holds.

We check (i)–(vi). Since $\mathrm{ord}(y-1) = \mathrm{ord}(\hat{u}-1)$ satisfies (xi), one sees easily from the inequalities of Theorem 4.6 that (ii), (iv) and (vi) hold. As for the others:

(i): $\mathrm{ord}(u-1) = \mathrm{ord}(\hat{y}-1) = e'/p = i' + r \geq i' + j/p$ since $j \leq 2r$.

(v): If $\mathrm{ord}(w\zeta_2 - 1) = \mathrm{ord}(z-1) = j' + t < e'/p$, then $j' + t \geq j'/p + k$ follows from

$$(p-1)j' \geq (p-1)i' \geq p(j-r) + p(k-t) \geq p(k-t).$$

If $\mathrm{ord}(w\zeta_2 - 1) = \mathrm{ord}(z-1) \geq e'/p$, then (v) follows from $e' = j' + j > j' + pk$.

(iii): To show $\mathrm{ord}(v^p\zeta_2 - 1) \geq i' + pk$, we observe that $e' > \mathrm{ord}(\hat{z}-1)$ and $e' > \mathrm{ord}(1-y)$, hence by Proposition 2.3,

$$\begin{aligned} \mathrm{ord}(G(\hat{u},\hat{z}) - 1) &= \mathrm{ord}(G(y,w) - 1) \\ &= \mathrm{ord}(y-1) + \mathrm{ord}(w-1) - e' \\ &\geq (\frac{p-1}{p})(e' + i' + k) \end{aligned}$$

by the assumption for (xi). We also have $\mathrm{ord}(x\zeta_3 - 1) = i' + s$, and so, since $vx\zeta_3 G(\hat{u},\hat{z}) = 1$, we have

$$\mathrm{ord}(v^p\zeta_2 - 1) \geq min\{pi' + ps, e'/p\}.$$

Now $(p-1)i' \geq p(k-s)$, so $pi' + ps \geq i' + pk$. Also, $e'/p = i' + r > i' + pk$. Thus all the inequalities hold, and so $H = J^*$ is a triangular Hopf order. □

5. Realizability and Hopf orders

For the moment we assume that H is an R-Hopf order in KG where G is an abelian group.

An *H-Galois algebra* is a finitely generated projective R-algebra A together with an H-module algebra structure $\beta : H \otimes_R A \to A$ for which the map

$$H \otimes A \to \mathrm{End}_R(A),$$

defined by $h \otimes x \mapsto (y \mapsto x \cdot \beta(h \otimes y))$, is bijective. The most interesting H-Galois algebras that one encounters are those which occur as rings of integers S of abelian extensions L/K with group G. In the terminology of C. Greither [Gr92], an R-Hopf order H in KG is *realizable as a Galois group*, or more simply, *realizable* if there exists a Galois extension L/K with group G for which S is an H-Galois algebra. If H is realizable via the extension L/K, then the module algebra map $\beta : H \otimes_R S \to S$ becomes just the classical Galois action $KG \otimes L \to L$ upon tensoring with K.

Greither [Gr92, Theorem II.3.2] has shown that $A(i,j,u)$, $j > 0$, is realizable if and only if p divides j and $\mathrm{ord}(u-1) = i' + (j/p)$.

Quite generally, N. Byott [By04] shows that a Hopf order H in KC_{p^n} with local dual H^* is realizable iff H^* is monogenic as an R-algebra.

Byott's result applies to the realizable Hopf orders of Greither. Thus the linear dual of the Greither order $A(i,j,u)$ with $j > 0$ and $pj \leq i$ must be monogenic.

Theorem 5.1. *Let $H = A(i,j,u)$ be an R-Hopf order in KC_{p^2} with* $\mathrm{ord}(u-1) = i' + (j/p)$. *Then $H^* = A(j',i',\hat{u})$ is monogenic with generator* $\dfrac{a_{\hat{u}}\gamma - 1}{\pi^{i'}}$.

Proof. From section 1 we know that the linear dual of $H = A(i,j,u)$ is the R-Hopf order $H^* = R\left[\frac{\gamma^p-1}{\pi^{j'}}, \frac{a_{\hat{u}}\gamma-1}{\pi^{i'}}\right]$. We claim that

$$R\left[\frac{a_{\hat{u}}\gamma-1}{\pi^{i'}}\right] = H^*.$$

Certainly $R\left[\frac{a_{\hat{u}}\gamma-1}{\pi^{i'}}\right] \subseteq H^*$ so it suffices to show that the generators of H^* are in $R\left[\frac{a_{\hat{u}}\gamma-1}{\pi^{i'}}\right]$. Evidently, we only need to show that

$$\frac{\gamma^p-1}{\pi^{j'}} \in R\left[\frac{a_{\hat{u}}\gamma-1}{\pi^{i'}}\right].$$

Put $\alpha = \frac{a_{\hat{u}}\gamma-1}{\pi^{i'}}$. Then

$$\alpha^p + \sum_{r=0}^{p-1}\binom{p}{r}\alpha^r\pi^{(p-r)i'} = \frac{a_{\hat{u}}^p\gamma^p-1}{\pi^{pi'}}.$$

Since $e' \geq i'$, the left-hand side of the above equation is in $R\left[\frac{a_{\hat{u}}\gamma-1}{\pi^{i'}}\right]$, hence,

$$R\left[\frac{a_{\hat{u}}^p\gamma^p-1}{\pi^{pi'}}\right] \subseteq R\left[\frac{a_{\hat{u}}\gamma-1}{\pi^{i'}}\right].$$

Now observe that

$$\frac{a_{\hat{u}}^p\gamma^p-1}{\pi^{pi'}} = \frac{a_{\hat{u}^p\zeta_1}-1}{\pi^{pi'}} = \frac{a_{u^{-p}}-1}{\pi^{pi'}}$$

with $\mathrm{ord}(u^{-p}-1) = \mathrm{ord}(u^p-1) = pi'+j = pi'+(j')'$, by hypothesis, hence

$$R\left[\frac{a_{\hat{u}}^p\gamma^p-1}{\pi^{pi'}}\right] = R\left[\frac{a_{u^{-p}}-1}{\pi^{pi'}}\right] = H(j'),$$

by Proposition 2.1. Therefore

$$H(j') \subseteq R\left[\frac{a_{\hat{u}}\gamma-1}{\pi^{i'}}\right],$$

and thus $\frac{\gamma^p-1}{\pi^{j'}} \in R\left[\frac{a_{\hat{u}}\gamma-1}{\pi^{i'}}\right]$. It follows that

$$H^* = R\left[\frac{a_{\hat{u}}\gamma-1}{\pi^{i'}}\right].$$ □

We now discuss the realizability of the Hopf orders in KC_{p^3} given in this paper.

Theorem 5.2. *An ILD Hopf order that is not cohomological is not realizable.*

Proof. Let $H = H(i,j,k,u,v,w)$ be an ILD Hopf order with $\mathrm{ord}(\hat{u}-1) < i'+j$, that is, H is an ILD Hopf order which is not cohomological. If H is realizable, then so is $\overline{H} = A(j,k,w)$, the image of H under the mapping $g^{p^2} \mapsto 1$. Thus $\mathrm{ord}(w-1) = j'+k/p < \varrho'+k/p$, which contradicts condition (C) of Proposition 1.8. □

Theorem 5.3. *No duality Hopf order is realizable.*

Proof. Suppose $H = H(i,j,k,u,v,w)$ is a realizable duality Hopf order. Then $\mathrm{ord}(u-1) = i' + j/p$ and $\mathrm{ord}(w-1) = j' + k/p$ by [Gr92, Lemma II.1.6]. Then $\mathrm{ord}(u^p - 1) = pi' + j$ since $i' + j/p < i' + i = e'$, and $pi' + j + j' + k/p = pi' + e' + k/p$. But inequality (x) of Theorem 3.7 requires

$$\mathrm{ord}(u^p - 1) + \mathrm{ord}(w-1) \geq pi' + e' + k.$$

This implies $k/p \geq k$, which is impossible. □

Theorem 5.4. *If $p > 2$, no formal group Hopf order H_Θ is realizable.*

Proof. Let $\overline{H} = A(j,k,w)$ denote the image of H_Θ under the mapping $g^{p^2} \mapsto 1$. Then the coalgebra structure of $\overline{H}$ is given by a 2-dimensional generically split polynomial formal group. Thus by [CU03, Theorem 3.0], $\mathrm{ord}(w-1) \geq j' + (k/2)$. Now if H_Θ is realizable, then so is $A(j,k,w)$, which is impossible. □

So we look at cohomological Hopf orders for realizability.

Theorem 5.5. *Let $H = H(i,j,k,\zeta_2^{-1},v,w)$, $k > 0$, be a cohomological Hopf order. If H is realizable, then $pi' = j'$.*

Proof. By [Gr92, Lemma II.1.6] we have $\mathrm{ord}(\zeta_2 - 1) = e'/p = i' + j/p$ which yields $pi' = j'$. □

So to find realizable cohomological Hopf orders we are restricted to the case $pi' = j'$. This subclass simplifies to the form

$$H(pi', i')^* \left[\frac{a_v b_{v^p} g - 1}{\pi^k} \right] = R \left[\frac{g^{p^2} - 1}{\pi^i}, \frac{a_{\zeta_2^{-1}} g^p - 1}{\pi^{(pi')'}}, \frac{a_v b_{v^p} g - 1}{\pi^k} \right],$$

with $v \in U_{i'+(k/p^2)} \cap U_{(i'/p)+k}$, $k > 0$ (cf. [CU03, Remark 4.1].

Underwood [Un98, Theorem 3.2.0], [Un03, Theorem 3.3.1] has shown that these cohomological Hopf orders are realizable if and only if p^2 divides k and $\mathrm{ord}(v-1) = i' + (k/p^2)$.

Hence by Byott's theorem, such Hopf orders must have monogenic duals.

Theorem 5.6. *Let $H = H(pi', i')^* \left[\frac{a_v b_{v^p} g - 1}{\pi^k} \right]$ be a cohomological Hopf order with $k > 0$, $\mathrm{ord}(v-1) = i' + (k/p^2)$, where p^2 divides k. Then*

$$H^* = R \left[\frac{\gamma^{p^2} - 1}{\pi^{k'}}, \frac{a_{\hat{v^p}} \gamma^p - 1}{\pi^{pi'}}, \frac{a_{\hat{v}} \gamma - 1}{\pi^{i'}} \right],$$

where $\hat{v^p} = (v^p \zeta_2)^{-1}$, and $\hat{v} = (v\zeta_3)^{-1}$, and H^* is monogenic with generator $\frac{a_{\hat{v}}\gamma - 1}{\pi^{i'}}$.

Proof. We first show that the dual H^* is of the claimed form.

By Theorem 4.8, we only need to show that $\langle H, J \rangle \subseteq R$, where

$$J = R \left[\frac{\gamma^{p^2} - 1}{\pi^{k'}}, \frac{a_{\hat{v^p}} \gamma^p - 1}{\pi^{pi'}}, \frac{a_{\hat{v}} \gamma - 1}{\pi^{i'}} \right],$$

and for this it suffices to show that

$$\mathrm{ord}(\langle (g^{p^2}-1)^q (a_{\zeta_2^{-1}} g^p - 1)^r (a_v b_{v^p} g - 1)^s, a_x \gamma - 1\rangle_3) \geq qi + r(pi')' + sk + i',$$

for $q, r, s = 0, \ldots, p-1$, where $x = \hat{\hat{v}}$. Put

$$\eta = \langle (g^{p^2}-1)^q (a_{\zeta_2^{-1}} g^p - 1)^r (a_v b_{v^p} g - 1)^s, a_x \gamma - 1\rangle_3.$$

Then

$$\begin{aligned}
\eta &= \sum_{c,d,e,\delta=0}^{q,r,s,1} C(c,d,e,\delta) \langle g^{p^2 c} a_{\zeta_2^{-d}} g^{pd} a_{v^e} b_{(v^p)^e} g^e, a_{x^\delta} \gamma^\delta \rangle_3 \\
&= \sum_{c,d,e,\delta=0}^{q,r,s,1} C(c,d,e,\delta) \langle g^{p^2 c + pd + e} a_{\zeta_2^{-d} v^e} b_{(v^p)^e}, \gamma^\delta a_{x^\delta} \rangle_3 \\
&= \sum_{c,d,e,\delta=0}^{q,r,s,1} C(c,d,e,\delta) \Gamma,
\end{aligned}$$

where

$$C(c,d,e,\delta) = \binom{q}{c}\binom{r}{d}\binom{s}{e}\binom{1}{\delta}(-1)^{q-c}(-1)^{r-d}(-1)^{s-e}(-1)^{1-\delta}$$

and

$$\Gamma = \sum_{pa+b, pm+n} \zeta_2^{-db} v^{eb} (v^p)^{ae} x^{\delta n} \langle e_{pa+b} g^{p^2 c + pd + e}, \hat{e}_{pm+n} \gamma^\delta \rangle_3.$$

By Lemma 3.4,

$$\langle e_{pa+b} g^{p^2 c + pd + e}, \hat{e}_{pm+n} \gamma^\delta \rangle_3 = \frac{1}{p} \zeta_1^{-a(m-d)} \zeta_3^{\delta(p^2 c + pd + e)} \delta_{e,n} \delta_{b,\delta}$$

so since $vx\zeta_3 = 1$ we have

$$\begin{aligned}
\Gamma &= \frac{1}{p} \sum_{a,m=0}^{p-1} \zeta_2^{-d\delta} v^{e\delta} (v^p)^{ae} x^{\delta e} \zeta_1^{-a(m-d)} \zeta_3^{\delta(p^2 c + pd + e)} \\
&= \zeta_1^{c\delta} \left(\frac{1}{p} \sum_{a,m=0}^{p-1} \zeta_1^{-a(m-d)} (v^{pe})^a \right) \\
&= \zeta_1^{c\delta} \left(\frac{1}{p} \sum_{a,m=0}^{p-1} \zeta_1^{-am} (v^{pe} \zeta_1^d)^a \right) \\
&= \zeta_1^{c\delta}.
\end{aligned}$$

So it suffices that

$$\eta = \sum_{c,d,e,\delta=0}^{q,r,s,1} C(c,d,e,\delta) \zeta_1^{c\delta} \in \pi^{qi + r(pi')' + sk + i'} R.$$

Since this last sum is equal to

$$\left(\sum_{d,e=0}^{r,s} \binom{r}{d}\binom{s}{e}(-1)^{r-d}(-1)^{s-e} \right) \left(\sum_{c,\delta=0}^{q,1} C(c,\delta) \zeta_1^{c\delta} \right),$$

and the first factor is 1 if $r, s = 0$, and 0 otherwise, it suffices to show that

$$\sum_{c,\delta=0}^{q,1} C(c,\delta)\zeta_1^{c\delta} \in \pi^{qi+i'}R,$$

for $q = 0, \ldots, p-1$, which clearly holds. Thus by Theorem 4.8, one has

$$H^* = R\left[\frac{\gamma^{p^2}-1}{\pi^{k'}}, \frac{a_{\hat{v^p}}\gamma^p - 1}{\pi^{pi'}}, \frac{a_{\hat{v}}\gamma - 1}{\pi^{i'}}\right].$$

We claim that $H^* = R\left[\frac{a_{\hat{v}}\gamma-1}{\pi^{i'}}\right]$. Certainly

$$R\left[\frac{a_{\hat{v}}\gamma - 1}{\pi^{i'}}\right] \subseteq H^*,$$

so it suffices to show that

$$H^* \subseteq R\left[\frac{a_{\hat{v}}\gamma - 1}{\pi^{i'}}\right],$$

and for this it suffices to show that each generator of H^* is in $R\left[\frac{a_{\hat{v}}\gamma-1}{\pi^{i'}}\right]$.

Since $e' \geq pi'$, $R\left[\frac{a_{\hat{v}^p}\gamma^p-1}{\pi^{pi'}}\right] \subseteq R\left[\frac{a_{\hat{v}}\gamma-1}{\pi^{i'}}\right]$, so it suffices to show that

$$R\left[\frac{a_{\hat{v}^p}\gamma^p - 1}{\pi^{pi'}}\right] = R\left[\frac{\gamma^{p^2}-1}{\pi^{k'}}, \frac{a_{\hat{v^p}}\gamma^p - 1}{\pi^{pi'}}\right],$$

which follows if we can show that

$$disc\left(R\left[\frac{a_{\hat{v}^p}\gamma^p - 1}{\pi^{pi'}}\right]\right) = disc\left(R\left[\frac{\gamma^{p^2}-1}{\pi^{k'}}, \frac{a_{\hat{v^p}}\gamma^p - 1}{\pi^{pi'}}\right]\right).$$

We show that the discriminants above are equal by extending the discriminant argument of Proposition 2.1. We have

$$disc\left(R\left[\frac{\gamma^{p^2}-1}{\pi^{k'}}, \frac{a_{\hat{v^p}}\gamma^p - 1}{\pi^{pi'}}\right]\right) = \left(\frac{p^2}{(p-1)(k'+pi')}\right)^{p^2},$$

by [Gr92, Lemma I.1.3a] and [La76]. Hence

$$\begin{aligned}\operatorname{ord}\left(disc\left(R\left[\frac{\gamma^{p^2}-1}{\pi^{k'}}, \frac{a_{\hat{v^p}}\gamma^p - 1}{\pi^{pi'}}\right]\right)\right) &= p^2(2e - (p-1)(k'+pi')) \\ &= p^2(p-1)(k + (pi')').\end{aligned}$$

On the other hand,

$$\begin{aligned}&disc\left(R\left[\frac{a_{\hat{v}^p}\gamma^p - 1}{\pi^{pi'}}\right]\right) \\ &\quad= \frac{1}{\pi^{p^2(p^2-1)pi'}} disc\left(1, a_{\hat{v}^p}\gamma^p - 1, (a_{\hat{v}^p}\gamma^p - 1)^2, \ldots, (a_{\hat{v}^p}\gamma^p - 1)^{p^2-1}\right) \\ &\quad= \frac{1}{\pi^{p^2(p^2-1)pi'}} disc\left(1, a_{\hat{v}^p}\gamma^p, (a_{\hat{v}^p}\gamma^p)^2, \ldots, (a_{\hat{v}^p}\gamma^p)^{p^2-1}\right) \\ &\quad= \frac{1}{\pi^{p^2(p^2-1)pi'}} disc\left(1, a_{\hat{v}^p\zeta_2}b_{\zeta_1}, (a_{\hat{v}^p\zeta_2}b_{\zeta_1})^2, \ldots, (a_{\hat{v}^p\zeta_2}b_{\zeta_1})^{p^2-1}\right) \\ &\quad= \frac{1}{\pi^{p^2(p^2-1)pi'}} disc\left(1, a_{v^{-p}}b_{\zeta_1}, (a_{v^{-p}}b_{\zeta_1})^2, \ldots, (a_{v^{-p}}b_{\zeta_1})^{p^2-1}\right).\end{aligned}$$

Now

$$(a_{v^{-p}}b_{\zeta_1})^k = \sum_{pm+n=0}^{p^2-1} (v^{-pn}\zeta_1^m)^k e_{pm+n},$$

for $0 \leq k \leq p^2-1$.

So

$$\begin{pmatrix} 1 \\ a_{\hat{v}^p}\gamma^p \\ (a_{\hat{v}^p}\gamma^p)^2 \\ \vdots \\ (a_{\hat{v}^p}\gamma^p)^{p^2-1} \end{pmatrix} = M \begin{pmatrix} e_0 \\ e_1 \\ e_2 \\ \vdots \\ e_{p^2-1} \end{pmatrix},$$

where M is the $p^2 \times p^2$ matrix whose $(pm+n+1)$st column, $0 \leq m, n \leq p-1$, is

$$\begin{pmatrix} 1 \\ v^{-pn}\zeta_1^m \\ (v^{-pn}\zeta_1^m)^2 \\ (v^{-pn}\zeta_1^m)^3 \\ \vdots \\ (v^{-pn}\zeta_1^m)^{p^2-1} \end{pmatrix}.$$

Since

$$disc(e_0, e_1, \ldots, e_{p^2-1}) = R,$$

it suffices to compute $(\det(M))^2$. Since M is Vandermonde,

$$\det(M) = \prod_{0 \leq pm+n < pm'+n' \leq p^2-1} (v^{-pn'}\zeta_1^{m'} - v^{-pn}\zeta_1^m).$$

But

$$\operatorname{ord}(v^{-pn'}\zeta_1^{m'} - v^{-pn}\zeta_1^m) = \operatorname{ord}(\zeta_1 - 1) = e'$$

if $n = n'$, and

$$\operatorname{ord}(v^{-pn'}\zeta_1^{m'} - v^{-pn}\zeta_1^m) = \operatorname{ord}(v^p - 1) = pi' + (k/p),$$

for all other cases, thus,

$$\operatorname{ord}(\det(M)) = \left(\frac{p^2(p-1)}{2}\right)e' + \left(\frac{p^2(p^2-1)}{2} - \frac{p^2(p-1)}{2}\right)(pi' + (k/p)),$$

and so

$$\begin{aligned} \operatorname{ord}\left(disc\left(R\left[\frac{a_{\hat{v}^p}\gamma^p - 1}{\pi^{pi'}}\right]\right)\right) &= p^2(p-1)e' + (p^2(p^2-1) \\ &\qquad -p^2(p-1))(pi' + (k/p)) - p^2(p^2-1)pi' \\ &= p^2(p-1)(pi')' + p^2(p-1)k \\ &= \operatorname{ord}\left(disc\left(R\left[\frac{\gamma^{p^2}-1}{\pi^{k'}}, \frac{a_{\hat{v^p}}\gamma^p - 1}{\pi^{pi'}}\right]\right)\right), \end{aligned}$$

which completes the proof. □

We seek other Hopf orders in KC_{p^3} which are realizable. From Byott's theorem, we need only construct a Hopf order H which is monogenic; then H^* will be realizable.

Let $A(p^2k,k,v) = R\left[\frac{g^{p^2}-1}{\pi^{p^2k}}, \frac{a_v g^p-1}{\pi^k}\right]$ be a Greither order, $\langle g^p\rangle = C_{p^2}$, with $\mathrm{ord}(v^p-1) > e'/p$, and set

$$A = R\left[\frac{g^{p^2}-1}{\pi^{p^2k}}, \frac{g^p-1}{\pi^{pk}}, \frac{a_v g-1}{\pi^k}\right].$$

Theorem 5.7. *The R-algebra A as above is a monogenic Hopf order with realizable linear dual*

$$A^* = R\left[\frac{\gamma^{p^2}-1}{\pi^{k'}}, \frac{a_{\zeta_2^{-1}}\gamma^p-1}{\pi^{(pk)'}}, \frac{a_{(v\zeta_3)^{-1}}b_{\zeta_2^{-1}}\gamma-1}{\pi^{(p^2k)'}}\right].$$

Proof. We first show that A is a Hopf order in KC_{p^3} using Proposition 1.1. We need $\frac{a_v^p g^p-1}{\pi^{pk}} \in H(p^2k,pk)$. To this end, write

$$\begin{aligned}\frac{a_v^p g^p-1}{\pi^{pk}} &= \frac{a_v^p g^p - a_v^p g^{p^2} + a_v^p g^{p^2}-1}{\pi^{pk}}\\ &= \frac{a_v^p g^p(1-g^{p^2-p})}{\pi^{pk}} + \frac{a_v^p g^{p^2}-1}{\pi^{pk}}.\end{aligned}$$

Now $\frac{a_v^p g^p(1-g^{p^2-p})}{\pi^{pk}} \in H(p^2k,pk)$ and $\frac{a_v^p g^{p^2}-1}{\pi^{pk}} \in H(p^2k)$ since $A(p^2k,k,v)$ is free over $H(p^2k)$ with basis $\{(\frac{a_v g^p-1}{\pi^k})^j\}$. Now since a_v is a unit in $A(p^2k,k,v)$, it suffices to show that

$$\Delta(a_v) \equiv a_v \otimes a_v \pmod{\pi^k(A(p^2k,k,v)\otimes A(p^2k,k,v))}.$$

But this follows from [C00, (31.10)] since $\mathrm{ord}(v^p-1) \geq p(p^2k)' + k$ by Theorem 1.5. Thus A is an Hopf order.

We claim that A is monogenic, generated by $\frac{a_v g-1}{\pi^k}$. Clearly $R\left[\frac{a_v g-1}{\pi^k}\right] \subseteq A$. So it remains to show that $A \subseteq R\left[\frac{a_v g-1}{\pi^k}\right]$. Since $e' \geq k$, $R\left[\frac{a_v^p g^p-1}{\pi^{pk}}\right] \subseteq R\left[\frac{a_v g-1}{\pi^k}\right]$, so it suffices to show that $R\left[\frac{a_v^p g^p-1}{\pi^{pk}}\right] = R\left[\frac{g^{p^2}-1}{\pi^{p^2k}}, \frac{g^p-1}{\pi^{pk}}\right]$. Since A is Hopf, $R\left[\frac{a_v^p g^p-1}{\pi^{pk}}\right] \subseteq R\left[\frac{g^{p^2}-1}{\pi^{p^2k}}, \frac{g^p-1}{\pi^{pk}}\right]$.

Now

$$disc\left(R\left[\frac{g^{p^2}-1}{\pi^{p^2k}}, \frac{g^p-1}{\pi^{pk}}\right]\right) = \left(\frac{p^2}{(p-1)(p^2k+pk)}\right)^{p^2},$$

Hence

$$\begin{aligned}&\mathrm{ord}\left(disc\left(R\left[\frac{g^{p^2}-1}{\pi^{p^2k}}, \frac{g^p-1}{\pi^{pk}}\right]\right)\right)\\ &\qquad = p^2(2e-(p-1)(p^2k+pk)) = p^2(p-1)((p^2k)' + (pk)').\end{aligned}$$

On the other hand,

$$\begin{aligned}\operatorname{ord}\left(\operatorname{disc}\left(R\left[\frac{a_v^p g^p-1}{\pi^{pk}}\right]\right)\right) &= p^2(p-1)(e'+p\operatorname{ord}(v^p\zeta_2-1))-p^2(p^2-1)pk\\ &= p^2(p-1)(e'+p\operatorname{ord}(v^p\zeta_2-1)-(p+1)pk)\\ &= p^2(p-1)(2e'-(p+1)pk)\\ &= p^2(p-1)((p^2k)'+(pk)'),\end{aligned}$$

since $\operatorname{ord}(v^p-1)>e'/p$. Thus A is monogenic.

We next compute A^*. Put

$$J=R\left[\frac{\gamma^{p^2}-1}{\pi^{k'}},\frac{a_{\zeta_2^{-1}}\gamma^p-1}{\pi^{(pk)'}},\frac{a_{(v\zeta_3)^{-1}}b_{\zeta_2^{-1}}\gamma-1}{\pi^{(p^2k)'}}\right].$$

By Theorem 4.8, we only need to show that $\langle A,J\rangle\subseteq R$, and for this it suffices to show that

$$\operatorname{ord}(\langle(g^{p^2}-1)^q(g^p-1)^r(a_vg-1)^s,a_xb_y\gamma-1\rangle_3)\geq qp^2k+rpk+sk+(p^2k)',$$

for $q,r,s=0,\dots,p-1$, where $x=\hat{\hat{v}}$, $y=\zeta_2^{-1}$. Put

$$\eta=\langle(g^{p^2}-1)^q(g^p-1)^r(a_vg-1)^s,a_xb_y\gamma-1\rangle_3.$$

Then

$$\begin{aligned}\eta &= \sum_{c,d,e,\delta=0}^{q,r,s,1}C(c,d,e,\delta)\langle g^{p^2c}g^{pd}a_{v^e}g^e,a_{x^\delta}b_{y^\delta}\gamma^\delta\rangle_3\\ &= \sum_{c,d,e,\delta=0}^{q,r,s,1}C(c,d,e,\delta)\langle g^{p^2c+pd+e}a_{v^e},\gamma^\delta a_{x^\delta}b_{y^\delta}\rangle_3\\ &= \sum_{c,d,e,\delta=0}^{q,r,s,1}C(c,d,e,\delta)\Gamma,\end{aligned}$$

where

$$C(c,d,e,\delta)=\binom{q}{c}\binom{r}{d}\binom{s}{e}\binom{1}{\delta}(-1)^{q-c}(-1)^{r-d}(-1)^{s-e}(-1)^{1-\delta}$$

and

$$\Gamma=\sum_{pa+b,pm+n}v^{eb}x^{\delta n}y^{m\delta}\langle e_{pa+b}g^{p^2c+pd+e},\hat{e}_{pm+n}\gamma^\delta\rangle_3.$$

By Lemma 3.4,

$$\langle e_{pa+b}g^{p^2c+pd+e},\hat{e}_{pm+n}\gamma^\delta\rangle_3=\frac{1}{p}\zeta_1^{-a(m-d)}\zeta_3^{\delta(p^2c+pd+e)}\delta_{e,n}\delta_{b,\delta}$$

so since $y\zeta_2 = 1$, $vx\zeta_3 = 1$ we have

$$\begin{aligned}
\Gamma &= \frac{1}{p}\sum_{a,m=0}^{p-1} v^{e\delta}x^{\delta e}y^{m\delta}\zeta_1^{-a(m-d)}\zeta_3^{\delta(p^2c+pd+e)} \\
&= \frac{1}{p}\sum_{a,m=0}^{p-1} \zeta_2^{-m\delta}\zeta_1^{-am}\zeta_1^{ad}\zeta_1^{c\delta}\zeta_2^{d\delta} \\
&= \zeta_1^{c\delta}\zeta_2^{d\delta}\frac{1}{p}\sum_{a,m=0}^{p-1}\zeta_1^{-am}(\zeta_2^{-\delta})^m(\zeta_1^d)^a \\
&= \zeta_1^{c\delta}\zeta_2^{d\delta}G(\zeta_2^{-\delta},\zeta_1^d) \\
&= \zeta_1^{c\delta}.
\end{aligned}$$

So it suffices that

$$\eta = \sum_{c,d,e,\delta=0}^{q,r,s,1} C(c,d,e,\delta)\zeta_1^{c\delta} \in \pi^{qp^2k+rpk+sk+(p^2k)'}R.$$

Since this last sum is equal to

$$\left(\sum_{d,e=0}^{r,s}\binom{r}{d}\binom{s}{e}(-1)^{r-d}(-1)^{s-e}\right)\left(\sum_{c,\delta=0}^{q,1}C(c,\delta)\zeta_1^{c\delta}\right),$$

and the first factor is 1 is $r,s=0$ and 0 otherwise, it suffices to show that

$$\sum_{c,\delta=0}^{q,1} C(c,\delta)\zeta_1^{c\delta} \in \pi^{qp^2k+(p^2k)'}R,$$

for $q = 0,\ldots,p-1$, which holds. Thus by Theorem 4.8, one has

$$A^* = R\left[\frac{\gamma^{p^2}-1}{\pi^{k'}}, \frac{a_{\zeta_2^{-1}}\gamma^p - 1}{\pi^{(pk)'}}, \frac{a_{(v\zeta_3)^{-1}}b_{\zeta_2^{-1}}\gamma - 1}{\pi^{(p^2k)'}}\right].$$

□

The realizable Hopf orders of Theorem 5.6 and Theorem 5.7 are distinct as the following example shows.

Example 5.8. Set $p=3$, $e'=300$, $k=30$, $\mathrm{ord}(v-1)=40$. Then

$$A = R\left[\frac{g^9-1}{\pi^{270}}, \frac{g^3-1}{\pi^{90}}, \frac{a_v g - 1}{\pi^{30}}\right]$$

is a monogenic R-Hopf order in KC_{27} with realizable linear dual

$$A^* = R\left[\frac{\gamma^9-1}{\pi^{270}}, \frac{a_{\zeta_2^{-1}}\gamma^3-1}{\pi^{210}}, \frac{a_{(v\zeta_3)^{-1}}b_{\zeta_2^{-1}}\gamma-1}{\pi^{30}}\right].$$

Note $\mathcal{L}\left(R\left[\frac{\gamma^9-1}{\pi^{270}}, \frac{a_{\zeta_2^{-1}}\gamma^3-1}{\pi^{210}}\right]\right) = H(270,70)$. But $3(30) \not\leq 70$, so A^* cannot be of the form of Theorem 5.6.

Remark 5.9. Let $A_0 = A(p^2k, k, v)$ and $A = H(p^2k, pk, k, 1, v, 1)$ be the Hopf orders of Theorem 5.7, and assume $p^2k < e'$ and $\mathrm{ord}(v^p - 1) = b$ with $e' > b > e'/p$. We show that for suitable choice of k, A^* is not an ILD order, not a formal group Hopf order, not the dual of a formal group Hopf order, and not a duality Hopf order. Thus A^* is not any of the types constructed earlier in this paper.

To show that A^* cannot be an ILD Hopf order, we first draw consequences from the fact that A_0 is Greither. Since $\mathrm{ord}(v^p\zeta_1 - 1) = b$, we have

$$b \geq e' - p^2k + pk, \tag{5}$$

$$b \geq p(e' - p^2k) + k. \tag{6}$$

Since $b < e'$, (6) implies

$$p^3k - k \geq pe' - e',$$

Hence

$$p^2k \geq \left(\frac{p^3 - p^2}{p^3 - 1}\right) e'. \tag{7}$$

Now $A^* = A(k', (pk)', (p^2k)', \zeta_2^{-1}, (v\zeta_3)^{-1}, \zeta_2^{-1})$ is an extension of a rank p Larson order by a Larson dual. Hence if A^* is ILD, then A^* is cohomological. For that to occur, we require conditions on the valuation parameters, namely

$$p(e' - p^2k) \leq e' - pk, \tag{8}$$

which implies

$$p^2k \geq \left(\frac{p^3 - p^2}{p^3 - p}\right) e'$$

and

$$k + p(e' - p^2k) \leq e'/p, \tag{9}$$

which implies

$$p^2k \geq \left(\frac{p^3 - p}{p^3 - 1}\right) e'.$$

Thus, recalling (7), if

$$\left(\frac{p^3 - p^2}{p^3 - 1}\right) e' \leq p^2k < \left(\frac{p^3 - p^2}{p^3 - p}\right) e' < \left(\frac{p^3 - p}{p^3 - 1}\right) e',$$

then A^* is not cohomological. As an example, for $p = 3$, $e' = 780, k = 61$, then $(18/26)e' = 540 < 9k = 549 < (18/24)e' = 585$.

Also, A^* is not a formal group Hopf order. To be a formal group Hopf order, we would require that $(pk)' \geq p(p^2k)'$, hence

$$p^2k \geq \left(\frac{p^3 - p^2}{p^3 - p}\right) e',$$

hence the last example fails this inequality and A^* is not a formal group Hopf order.

Neither can A^* be the dual of a formal group Hopf order as constructed in Theorem 4.1 or Theorem 4.6. For suppose A is a formal group Hopf order, $A = H_\Theta$. Then Θ must have the form

$$\Theta = \begin{pmatrix} \pi^{p^2k} & 0 & 0 \\ 0 & \pi^{pk} & 0 \\ c\pi^s & 0 & \pi^k \end{pmatrix}.$$

Then A is not a formal group Hopf order as in Theorem 4.1 because there we require that $\mathrm{ord}(\theta_{r,r}) \geq d\,\mathrm{ord}(\theta_{r+1,r+1})$ with $d > p$. Moreover, A is not of the form of Theorem 4.6 since there we require that b and d be units of R.

The construction of Theorem 4.6 remains valid in the case that $b = d = 0$, however, and the resulting formal group Hopf orders H_Θ have matrices of the form Θ with $2s \geq k > s$, and c a unit. We show that there exists A not of the form H_Θ. If $A = H_\Theta$, then $\langle H_\Theta, A^* \rangle \subset R$, so in particular,

$$\left\langle \frac{g-1}{\pi^k} + \frac{-c\pi^s(g^{p^2}-1)}{\pi^{p^2k+k}}, \frac{a_{(v\zeta_3)^{-1}} b_{\zeta_2^{-1}} \gamma - 1}{\pi^{(p^2k)'}} \right\rangle \in R.$$

But the expression in angle brackets is

$$\frac{v^{-1}-1}{\pi^{(p^2k)'+k}} + \frac{-c\pi^{s-p^2k}}{\pi^{(p^2k)'+k}}(\zeta_1 - 1),$$

so we require that

$$v^{-1} \equiv 1 + c\pi^{s-p^2k}(\zeta_1 - 1) \pmod{\pi^{(p^2k)'+k}R}.$$

Since $(p^2k)' + s < (p^2k)' + k$, $\mathrm{ord}(1-v) = (p^2k)' + s$, hence we require that $\mathrm{ord}(1-v) \geq (p^2k)' + (k/2)$. Now since $e'/p > \mathrm{ord}(1-v)$, any k for which $(p^2k)' + (k/2) > e'/p$ yields A is not a formal group. In fact, the example given earlier provides such a k.

Finally, since $\mathrm{ord}(1-v^p) > e'/p$, A is monogenic, hence A^* is realizable. Thus neither A^* nor A can be duality by Theorem 5.3.

References

[By93] N. Byott, Cleft extensions of Hopf algebras, *Proc. London Math. Soc.* **67** (1993), 227-307. MR1226603 (94m:16044)

[By02a] N. Byott, Integral Hopf-Galois structures in degree p^2 extensions of p-adic fields, *J. Alg.*, **248** (2002), 334-365. MR1879021 (2002j:11142)

[By04] N. Byott, Monogenic Hopf orders and associated orders of valuation rings, J. Algebra **275** (2004), 575–599. MR2052627

[C96] L. N. Childs, Hopf Galois structures on degree p^2 cyclic extensions of local fields, *New York J. of Math.*, **2** (1996), 86-102. MR1420597 (97j:11058)

[C98] L. N. Childs, Introduction to polynomial formal groups and Hopf algebras, Memoirs Am. Math. Soc., **136**, no. 651 (1998), 1-10. MR1629460 (2000c:14067)

[C00] L. N. Childs, Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory, American Mathematical Society, Mathematical Surveys and Monographs **80**, 2000. MR1767499 (2001e:11116)

[CMS98] L. N. Childs, D.J. Moss, J. Sauerberg, Dimension one polynomial formal groups, Memoirs Am. Math. Soc., **136**, no. 651 (1998), 11-19. MR1629460 (2000c:14067)

[CMSZ98] L. N. Childs, D.J. Moss, J. Sauerberg, K. Zimmermann, Dimension two polynomial formal groups, Memoirs Am. Math. Soc., **136**, no. 651 (1998), 21-54. MR1629460 (2000c:14067)

[CS98] L.N. Childs, J. Sauerberg, Degree two formal groups and Hopf algebras, Memoirs Amer. Math. Soc., **136**, no. 651 (1998), 55-89. MR1629460 (2000c:14067)

[CU03] L. N. Childs, R.G. Underwood, Cyclic Hopf orders defined by isogenies of formal groups, *Amer. J. Math.*, **125** (2003), 1295-1334. MR2018662 (2004i:11138)

[CZ94] L. N. Childs, K. Zimmermann, Congruence-torsion subgroups of dimension one formal groups, *J. Alg.*, **170** (1994), 929-955. MR1305271 (95k:14067)

[Gr92] C. Greither, Extensions of finite group schemes, and Hopf Galois theory over a complete discrete valuation ring, *Math. Z.*, **210** (1992), 37-67. MR1161169 (93f:14024)

[GC98] C. Greither, L. N. Childs, p-elementary group schemes–constructions, and Raynaud's theory, Memoirs Am. Math. Soc., **136**, no. 651 (1998), 91-117. MR1629460 (2000c:14067)

[La76] R. G. Larson, Hopf algebra orders determined by group valuations, *J. Alg.*, **38** (1976), 414-452. MR0404413 (53:8215)

[Lu79] J. Lubin, Canonical subgroups of formal groups, *Trans. Am. Math. Soc.*, **251** (1979), 103-127. MR0531971 (80j:14039)

[Sm97] H. Smith, Constructing Hopf orders in elementary abelian group rings, doctoral dissertation, SUNY Albany (1997).

[SS94] T. Sekiguchi, N. Suwa, Theories de Kummer-Artin-Schreier-Witt, *Comptes Rendus de l'Acad. des Sci.*, **319**, ser. I (1994), 105-110. MR1288386

[TO70] F. Tate, J. Oort, Group schemes of prime order, *Ann. Sci. Ec. Norm. Sup.*, **3** (1970), 1-21. MR0265368 (42:278)

[Un94] R. Underwood, R-Hopf algebra orders in KC_{p^2}, *J. Alg.*, **169** (1994), 418-440. MR1297158 (95k:16055)

[Un96] R. Underwood, The valuative condition and R-Hopf algebra orders in KC_{p^3}, *Amer. J. Math.*, **118** (1996), 401-743. MR1400057 (97e:11150)

[Un98] R. Underwood, The structure and realizability of R-Hopf orders in KC_{p^3}, *Comm. Alg.*, **26**(11) (1998), 3447-3462. MR1647146 (2000a:16073)

[Un99] R. Underwood, Isogenies of polynomial formal groups, *J. Alg.*, **212** (1999), 428-459. MR1676848 (99m:14084)

[Un03] R. Underwood, Galois module theory over a discrete valuation ring, in "Recent Research on Pure and Applied Algebra", Nova Science Publishers, New York, 2003. MR2030462

Department of Mathematics, Auburn University Montgomery, Montgomery, Alabama 36124

Department of Mathematics and Statistics, SUNY at Albany, Albany, New York 12222