International Mathematical Forum, 1, 2006, no. 17, 833-851

REALIZABLE HOPF ORDERS in KC_8

Robert G. Underwood

Department of Mathematics
Auburn University Montgomery
Montgomery, AL 36124 USA
runderwo@mail.aum.edu

Abstract

Let K be a finite extension of the 2-adic rationals $\mathbb{Q}_2$ with ring of integers R. Let C_8 denote the cyclic group of order 8. In this paper we construct a new collection of realizable Hopf orders in the group ring KC_8.

Mathematics Subject Classification: 11R33, 11S15, 12F10, 16W30

Keywords: discrete valuation ring, cyclic group, Hopf order, realizability, Galois module theory

1. Introduction

Let p be a prime number and let K be a finite extension of the p-adic rationals $\mathbb{Q}_p$ containing ζ_n, $n \geq 1$, a primitive p^nth root of unity with $\zeta_n^p = \zeta_{n-1}$. Let $\mathrm{ord}(a)$ be the valuation of a in K normalized so that $\mathrm{ord}(\pi) = 1$ where π is a parameter of K. Let R denote the ring of integers of K and let $\mathrm{ord}(p) = e$ denote the ramification index of p in R. Put $e' = e/(p-1)$. For an integer m, $0 \leq m \leq e'$, set $m' = e' - m$, and for a unit $u \in R$, set $\tilde{u} = \zeta_2^{-1} u^{-1}$.

Let C_{p^n} denote the cyclic group of order p^n, generated by g, with character group $\hat{C}_{p^n}$, generated by γ. Let $\langle\ ,\ \rangle_n : K\hat{C}_{p^n} \times KC_{p^n} \to K$ denote the duality pairing defined by $\langle \gamma, g\rangle_n = \zeta_n$. When there is no chance of confusion we will use the simpler notation $\langle\ ,\ \rangle$.

It is well-known that KC_{p^n} can be endowed with the structure of a K-Hopf algebra via the comultiplication map $\Delta : KC_{p^n} \to KC_{p^n} \otimes KC_{p^n}$, defined by $g \mapsto g \otimes g$, the counit map $\varepsilon : KC_{p^n} \to K$, defined by $g \mapsto 1$, and the coinverse map $\sigma : KC_{p^n} \to KC_{p^n}$, given by $g \mapsto g^{-1}$.

Let H denote an R-Hopf algebra order in KC_{p^n}. Through the work of Tate and Oort [9], Larson [7], Greither [5], Byott [1], Underwood [10], Childs [3], and Underwood and Childs [13], the classification of Hopf (algebra) orders in KC_{p^n} is complete for the cases $n = 1, 2$. The classification for $n > 2$ is an open problem however, even for $n = 3$. In the case $n = 3$, large classes of Hopf orders have been constructed: R. Underwood and L. Childs have identified collections of *triangular*, *cohomological*, *ILD*, *duality* and *formal group* Hopf orders, see [11], [4], and [13]. Nevertheless, a complete classification remains elusive. We shall consider the case $n = 3$ in this paper.

A Hopf order $H \subseteq KC_{p^3}$ is *realizable* if there exists a Galois extension L/K with group C_{p^3} for which $S = \mathcal{O}_L$ is an H-Galois algebra, cf. [5]. The realizable Hopf orders constitute an important subclass of Hopf orders in KC_{p^3}. Unfortunately, most of these Hopf orders have yet to be found, cf. [13, §5]. And it is apparent that the complete classification for $n = 3$ will not be achieved until these remaining Hopf orders are constructed.

The purpose of this paper is to construct realizable Hopf orders in KC_8 ($p = 2$) which are distinct from all known realizable Hopf orders in KC_8. We are hopeful that our methods will generalize to odd primes in subsequent work.

2. Hopf orders in KC_8

For the remainder of this paper we fix $p = 2$ and $n = 3$. Then $e = e'$.

Let $\overline{g}$ denote the image of g under the mapping $C_8 \xrightarrow{g^4 \mapsto 1} C_4$; let $\overline{\gamma}$ denote the image of γ under the mapping $\hat{C}_8 \xrightarrow{\gamma^4 \mapsto 1} \hat{C}_4$.

Let

$$A(i, j, u) = R\left[\frac{g^4 - 1}{\pi^i}, \frac{g^2 a_u - 1}{\pi^j}\right],$$

and

$$A(j, k, w) = R\left[\frac{\overline{g}^2 - 1}{\pi^j}, \frac{\overline{g} a_w - 1}{\pi^k}\right]$$

be Hopf orders in KC_4 [3, §31]. By [10, Theorem 1.3.1], $i \geq j \geq k$. Moreover, $\mathrm{ord}(1-u) \geq i' + (j/2)$ and $\mathrm{ord}(1-w) \geq j' + (k/2)$, cf. [13, §1]. We assume that $k > 0$.

Since $\zeta_2 \in K$, the linear duals of these Hopf orders are Hopf orders in KC_4 of the form

$$A(i,j,u)^* = A(j',i',\tilde{u}) = R\left[\frac{\overline{\gamma}^2 - 1}{\pi^{j'}}, \frac{\overline{\gamma} a_{\tilde{u}} - 1}{\pi^{i'}}\right],$$

$$A(j,k,w)^* = A(k',j',\tilde{w}) = R\left[\frac{\gamma^4 - 1}{\pi^{k'}}, \frac{\gamma^2 a_{\tilde{w}} - 1}{\pi^{j'}}\right]$$

[13, Theorem 1.2].

Our goal is to extend the rank 4 Hopf order $A(i,j,u)$ to obtain a Hopf order of rank 8.

Let s, t, u_1, u_3 be units of R. Put

$$\beta = \iota_0 + s\iota_1 + \tilde{u}\iota_2 + t\iota_3$$

$$b = e_0 + u_1 e_1 + w e_2 + u_3 e_3,$$

where the ι_m, e_m are the minimal idempotents for $K\langle\gamma^2\rangle$ and $K\langle g^2\rangle$, respectively.

We seek values for u_1, u_3 so that

$$\big\langle (\gamma^4 - 1)^q (\gamma^2 a_{\tilde{w}} - 1)^r (\gamma\beta - 1), gb - 1 \big\rangle = 0, \tag{1}$$

for $q, r = 0, 1$.

Set $c = (s+t)/2$, $d = (s-t)/2$. Using [13, Theorem 3.7], (1) reduces to the linear system,

$$\begin{cases} \zeta_3(u_1 c + u_3 d) - 1 = 0 \\ \tilde{w}\zeta_2\zeta_3(u_1 d + u_3 c) - \zeta_3(u_1 c + u_3 d) = 0, \end{cases}$$

which has the unique solution

$$u_1 = \frac{wd - c}{\zeta_3(d^2 - c^2)}, \quad u_3 = \frac{d - wc}{\zeta_3(d^2 - c^2)}.$$

So we put

$$b = \sum_{r=0}^{3} u_r e_r = e_0 + \left(\frac{wd - c}{\zeta_3(d^2 - c^2)}\right) e_1 + we_2 + \left(\frac{d - wc}{\zeta_3(d^2 - c^2)}\right) e_3.$$

Now let

$$A = A(i, j, u)\left[\frac{gb - 1}{\pi^k}\right]$$

denote the R-module which is the $A(i, j, u)$-span of the set $\left\{1, \frac{gb-1}{\pi^k}\right\}$, and let

$$G(m, n) = \frac{1 + n}{2} + m\left(\frac{1 - n}{2}\right)$$

denote the Gauss sum of m and n [6].

Lemma 2.1. *Let A be an R-module as in the previous text and suppose*

$$(a) \quad ord(s^{-1}t - \tilde{u}) \geq j + i';$$

$$(b) \quad ord\left(\zeta_2 s^2 G(-s^{-2}t^2, w) - 1\right) \geq k + 2i';$$

$$(c) \quad ord(\zeta_3 s - 1) \geq i' + \frac{k}{4}.$$

Then A is an R-coalgebra.

Proof. Since $A \subseteq KC_8$, the counit map $\varepsilon : KC_8 \to K$ induces a counit map on A.

We next show that the comultiplication $\Delta : KC_8 \to KC_8 \otimes KC_8$ induces a comultiplication on A.

From (a) and [5, Lemma 3.2b], $A(j', i', \tilde{u}) = A(j', i', s^{-1}t)$. We claim that b is a unit of $A(i, j, u)$. Since the u_m are units in R, this amounts to showing that $\langle A(j', i', s^{-1}t), b\rangle \subseteq R$.

We show that

(2) $$\operatorname{ord}\left(\left\langle(\overline{\gamma}^2-1)^l(\overline{\gamma}a_{s^{-1}t}-1)^m, b\right\rangle\right) \geq lj'+mi',$$

for $l, m \in 0, 1$. We have

$$\begin{aligned}
\langle(\overline{\gamma}^2-1)^l(\overline{\gamma}a_{s^{-1}t}-1)^m, b\rangle &= \sum_{\alpha=0}^{l}\sum_{\beta=0}^{m}\binom{l}{\alpha}\binom{m}{\beta}(-1)^{l-\alpha}(-1)^{m-\beta}\langle\overline{\gamma}^{2\alpha+\beta}a_{s^{-\beta}t^{\beta}}, b\rangle \\
&= \sum_{\alpha=0}^{l}\sum_{\beta=0}^{m}\binom{l}{\alpha}\binom{m}{\beta}(-1)^{l-\alpha}(-1)^{m-\beta}w^{\alpha}\zeta_3^{-\beta}s^{-\beta} \\
&= (1-w)^l(1-\zeta_3^{-1}s^{-1})^m.
\end{aligned}$$

Hence (2) follows by (c) and the condition $\operatorname{ord}(1-w) \geq j'+(k/2)$.

Put $\xi = \dfrac{gb-1}{\pi^k}$. Since

$$\Delta(\xi) = \xi\otimes 1 + 1\otimes\xi + \pi^k\xi\otimes\xi + \frac{\Delta(gb)-gb\otimes gb}{\pi^k},$$

A is a coalgebra if and only if $\dfrac{\Delta(gb)-gb\otimes gb}{\pi^k} \in A\otimes A$. Since b is a unit in $A(i,j,u)$, $g = (\pi^k\xi+1)b^{-1} \in A$. Thus

$$\frac{\Delta(gb)-gb\otimes gb}{\pi^k} = \left(\frac{\Delta(b)-b\otimes b}{\pi^k}\right)(g\otimes g) \in A\otimes A$$

if and only if

(3) $$\frac{\Delta(b)-b\otimes b}{\pi^k} \in A(i,j,u)\otimes A(i,j,u).$$

For integers l, m, n, q, put

$$\Omega = (\overline{\gamma}^2-1)^l(\overline{\gamma}a_{s^{-1}t}-1)^m \otimes (\overline{\gamma}^2-1)^n(\overline{\gamma}a_{s^{-1}t}-1)^q.$$

Now (3) holds if and only if

(4) $$\operatorname{ord}\left(\langle\Omega, \Delta(b)-b\otimes b\rangle\right) \geq (l+n)j' + (m+q)i' + k,$$

for $l, m, n, q = 0, 1$.

We consider the following cases in (4).

Case 1. $l+n<2$ and $m+q<2$. In this case,

$$\langle \Omega, \Delta(b) - b \otimes b \rangle = 0.$$

Case 2. $l + n = 2$ and $m + q < 2$. Here,

$$\langle \Omega, \Delta(b) - b \otimes b \rangle = (1 - w^2)(1 - \zeta_3^{-1} s^{-1})^{m+q},$$

Case 3. $l + n < 2$, $m + q = 2$. Then,

$$\langle \Omega, \Delta(b) - b \otimes b \rangle = (1 - w)^{l+n}(G(-s^{-2}t^2, w) - \zeta_2^{-1} s^{-2}) + Q,$$

where Q is an element of R with $\mathrm{ord}(Q) \geq (l+n)j' + 2i' + k$.

Case 4. $l + n = 2$, $m + q = 2$. Now,

$$\langle \Omega, \Delta(b) - b \otimes b \rangle = (1 - w^2)(1 - \zeta_3^{-1} s^{-1})^2 + M,$$

where M is an element of R with $\mathrm{ord}(M) \geq 2j' + 2i' + k$.

In each case, (4) holds using (b), (c) and the condition $\mathrm{ord}(1 - w^2) \geq 2j' + k$. □

Now suppose $A = A(i, j, u)\left[\dfrac{gb - 1}{\pi^k}\right]$ is a coalgebra as constructed by Lemma 2.1. Put

$$x = \frac{u_1 + u_3}{2} \quad \text{and} \quad y = \frac{u_1 - u_3}{2},$$

and set

$$v_0 = 1, \quad v_1 = \frac{\tilde{u}y - x}{\zeta_3(y^2 - x^2)}, \quad v_2 = \tilde{u}, \quad v_3 = \frac{y - \tilde{u}x}{\zeta_3(y^2 - x^2)}.$$

Let $\beta = \sum_{r=0}^{3} v_r \iota_r$ where the ι_r are the minimal idempotents of $K\hat{C}_4$. Let $B = A(k', j', \tilde{w})\left[\dfrac{\gamma\beta - 1}{\pi^{i'}}\right]$ denote the R-module which is the $A(k', j', \tilde{w})$-span of the set $\left\{1, \dfrac{\gamma\beta - 1}{\pi^{i'}}\right\}$.

Lemma 2.2. *Suppose $i \geq 2j$, $j' \geq 2i'$, $k' \geq 4i'$, $j \geq 4k$, and $e' \geq i + j + k$. Then the R-module B is an R-coalgebra.*

Proof. We use Lemma 2.1. In this case, B is a coalgebra if

$$\operatorname{ord}(u_1^{-1}u_3 - w) \geq j' + k; \tag{5}$$

$$\operatorname{ord}\left(\zeta_2 u_1^2 G(-u_1^{-2}u_3^2, \tilde{u}) - 1\right) \geq i' + 2k; \tag{6}$$

$$\operatorname{ord}(\zeta_3 u_1 - 1) \geq k + \frac{i'}{4}. \tag{7}$$

For (5), we show that $\operatorname{ord}(u_1 w - u_3) \geq j' + k$. To this end,

$$\frac{\overline{\gamma}^2 - 1}{\pi^{j'}} \in A(j', i', \tilde{u}) = A(i, j, u)^*,$$

thus

$$\pi^{-j'}(\overline{\gamma} \otimes \overline{\gamma}^2 - \overline{\gamma} \otimes 1) \in A(i, j, u)^* \otimes A(i, j, u)^*.$$

Since A is a coalgebra,

$$\pi^{-k}(\Delta(b) - b \otimes b) \in A(i, j, u) \otimes A(i, j, u),$$

hence

$$\begin{aligned} &\mu\left(\langle \pi^{-j'}(\overline{\gamma} \otimes \overline{\gamma}^2 - \overline{\gamma} \otimes 1), \pi^{-k}(\Delta(b) - b \otimes b)\rangle\right) \\ &\quad = \pi^{-k-j'}\mu\left(\langle \overline{\gamma} \otimes \overline{\gamma}^2, \Delta(b)\rangle - \langle \overline{\gamma} \otimes 1, \Delta(b)\rangle\right. \\ &\quad\qquad \left. - \langle \overline{\gamma} \otimes \overline{\gamma}^2, b \otimes b\rangle + \langle \overline{\gamma} \otimes 1, b \otimes b\rangle\right) \\ &\quad = \pi^{-k-j'}(u_3 - u_1 w) \in R \end{aligned}$$

or, $\operatorname{ord}(u_1 w - u_3) \geq j' + k$.

For (6), observe that

$$\begin{aligned} \zeta_3 u_1 &= \zeta_3\left(\frac{wd - c}{\zeta_3(d^2 - c^2)}\right) \\ &= s^{-1}\left(\frac{1 + w}{2}\right) + t^{-1}\left(\frac{1 - w}{2}\right) \\ &= s^{-1}G(st^{-1}, w). \end{aligned}$$

Note $\mathrm{ord}(\zeta_3 - 1) = (e'/4) \geq i' + (k/4)$, since $k' \geq 4i'$. So by condition (c) of Lemma 2.1, $\mathrm{ord}(s^{-1} - 1) \geq i' + (k/4)$. Since $e' \geq i + j + k$, $\mathrm{ord}(s^{-1} - 1) \geq (i'/2) + k$. Moreover,

$$\begin{aligned}\mathrm{ord}(G(st^{-1}, w) - 1) &= \mathrm{ord}(st^{-1} - 1) + \mathrm{ord}(1 - w) - e' \\ &\geq i' + (j/2) + j' + (k/2) - e' \\ &\geq \frac{i'}{2} + k\end{aligned}$$

since $j' \geq 2i'$, $e' \geq i + j + k$. Thus $\mathrm{ord}(\zeta_2 u_1^2 - 1) \geq i' + 2k$.

Also,

$$\begin{aligned}\mathrm{ord}(G(-u_1^{-2}u_3^2, \tilde{u}) - 1) &= \mathrm{ord}(G(\tilde{\omega}^{-2}, \tilde{u}) - 1), \quad \omega = u_1^{-1}u_3 \\ &= \mathrm{ord}(\tilde{\omega}^{-2} - 1) + \mathrm{ord}(1 - \tilde{u}) - e'.\end{aligned}$$

Suppose $\mathrm{ord}(\tilde{\omega}^{-2} - 1) < e'$. Then $\mathrm{ord}(1 - w) < e'/2$, which implies $k' \geq 2j'$, and ultimately, $k = 0$, which contradicts our assumption $k > 0$. Therefore, $\mathrm{ord}(\tilde{\omega}^{-2} - 1) \geq e'$. Now

$$\begin{aligned}\mathrm{ord}(G(-u_1^{-2}u_3^2, \tilde{u}) - 1) &\geq \mathrm{ord}(1 - \tilde{u}) \\ &\geq \frac{j}{2} + i' \\ &\geq i' + 2k,\end{aligned}$$

since $j' \geq 2i'$ and $j \geq 4k$. And so condition (6) holds.

Since $\mathrm{ord}(\zeta_3 u_1 - 1) \geq (i'/2) + k$, condition (7) follows.

□

We have the coalgebras $A = A(i, j, u)\left[\frac{gb - 1}{\pi^k}\right]$ and $B = A(k', j', \tilde{w})\left[\frac{\gamma\beta - 1}{\pi^{i'}}\right]$ as constructed above by Lemma 2.1 and Lemma 2.2.

Let

$$A^* = \{h \in K\hat{C}_8 | \langle h, A\rangle \subseteq R\}$$

denote the linear dual of A.

Lemma 2.3. *Let $\overline{A}$ be the image of A under the mapping $KC_8 \overset{g^4 \mapsto 1}{\to} KC_4$. Then*

$$K\hat{C}_4 \cap A^* = \overline{A}^* = A(j,k,w)^* = A(k',j',\tilde{w}).$$

Proof. We show that $\overline{A}^* = K\hat{C}_4 \cap A^*$. Let $\alpha \in \overline{A}^*$. Then $\alpha \in K\hat{C}_4$ and $\langle \alpha, \overline{A} \rangle_2 \subseteq R$. Let $f \in A$, and let $\overline{f}$ be the image of f under the mapping $KC_8 \overset{g^4 \mapsto 1}{\to} KC_4$. Then $\langle \alpha, f \rangle_3 = \langle \alpha, \overline{f} \rangle_2$. Hence

$$\langle \alpha, A \rangle_3 = \langle \alpha, \overline{A} \rangle_2 \subseteq R,$$

so that $\alpha \in A^*$. Hence $\alpha \in K\hat{C}_4 \cap A^*$.

Now suppose $\alpha \in K\hat{C}_4 \cap A^*$. Then $\alpha \in K\hat{C}_4$ and $\langle \alpha, A \rangle_3 \subseteq R$. Consequently, $\alpha \in \overline{A}^*$, which shows that $\overline{A}^* = K\hat{C}_4 \cap A^*$.

Since $\overline{b} = a_w$, $\overline{A} = A(j,k,w)$, which completes the proof of the lemma.

□

Lemma 2.4. *$B \subseteq A^*$.*

Proof. Since A^* is an algebra by [8, 1.2.2], it suffices to show that $A(k',j',\tilde{w}) \subseteq A^*$ and $\dfrac{\gamma\beta - 1}{\pi^{i'}} \in A^*$.

By Lemma 2.3, $A^* \cap K\hat{C}_4 = A(k',j',\tilde{w})$, thus $A(k',j',\tilde{w}) \subseteq A^*$. We claim that $\dfrac{\gamma\beta - 1}{\pi^{i'}} \in A^*$. But this amounts to showing that

$$\langle \gamma\beta - 1, A \rangle_3 \subseteq \pi^{i'} R.$$

Since $\dfrac{\gamma\beta - 1}{\pi^{i'}}$ acts on $A(i,j,u)$ as $\dfrac{\overline{\gamma} a_{\tilde{u}} - 1}{\pi^{i'}}$, it suffices to show that

$$\text{ord}\left(\langle \gamma\beta - 1, (g^4 - 1)^l (g^2 a_u - 1)^m (gb - 1) \rangle\right) \geq li + mj + k + i', \tag{8}$$

for $l, m = 0, 1$.

By [13, Theorem 3.7], (8) is equivalent to the system,

$$\begin{cases} \text{ord}(\zeta_3(v_1 x + v_3 y) - 1) \geq k + i' \\ \text{ord}(\zeta_3 u \zeta_2 (v_1 y + v_3 x) - \zeta_3(v_1 x + v_3 y)) \geq j + k + i', \end{cases}$$

which holds since $v_1 = \dfrac{\tilde{u} y - x}{\zeta_3(y^2 - x^2)}$ and $v_3 = \dfrac{y - \tilde{u} x}{\zeta_3(y^2 - x^2)}$.

□

Theorem 2.5. *The coalgebras* $A = A(i,j,u)\left[\frac{gb-1}{\pi^k}\right]$ *and* $B = A(k',j',\tilde{w})\left[\frac{\gamma\beta-1}{\pi^{i'}}\right]$ *are dual Hopf orders in* KC_8.

Proof. We first show that the coalgebra B is a Hopf order. It is easy to see that the coinverse map $\sigma : K\hat{C}_8 \to K\hat{C}_8$ induces a coinverse map on B.

So it remains to show that B is an algebra. Since A^* is an algebra with $A^* \cap K\hat{C}_4 = A(k',j',\tilde{w})$, $\frac{\gamma\beta-1}{\pi^{i'}} \in A^*$ satisfies a monic polynomial of degree 2 with coefficients in $A(k',j',\tilde{w})$. Thus B is an algebra as well as a coalgebra. Hence, B is an R-Hopf order.

Observe that $B \subseteq A^*$ implies $A \subseteq B^*$. Since $B^* \cap KC_4 = A(i,j,u)$ by Lemma 2.3, $\frac{gb-1}{\pi^k}$ satisfies a monic polynomial of degree 2 with coefficients in $A(i,j,u)$. Thus A is a Hopf order. A well-known discriminant argument then shows that $A^* = B$, see [13, §4].

□

3. Realizable Hopf orders in KC_8

In this section we use the results of §2 to construct a collection of realizable Hopf orders in KC_8.

Let $A(i,j,u)$ and $A(j,k,w)$ be Hopf orders in KC_4 with $k > 0$, $i \geq 2j$, $2|j$, and $4|k$. Put $w = 1+\pi^q$, $u = 1+\pi^l$, with $q = j' + (k/2)$ and $l = i' + (j/2)$. Let m be the smallest even integer $\geq 2i' + j + (k/2)$. Put $\nu = \zeta_3^{-1}(\zeta_2^{-1} - 1)$, so that $\nu^2 = 2$, and let

$$s = \zeta_3^{-1}\left(1 + \zeta_2\nu^{-1}\pi^{l+(q/2)}(1+\nu\pi^{-l/2})\right)^{-1},$$

and

$$t = \zeta_2\pi^{-q/2}\left(s(\nu + \pi^{q/2}) + \nu\zeta_2\zeta_3^{-1}(1+\pi^{m/2})\right).$$

Put $c = (s+t)/2$, $d = (s-t)/2$,

$$b = \sum_{r=0}^{3} u_r e_r = e_0 + \left(\frac{wd-c}{\zeta_3(d^2-c^2)}\right)e_1 + we_2 + \left(\frac{d-wc}{\zeta_3(d^2-c^2)}\right)e_3,$$

and $A = A(i,j,u)\left[\frac{gb-1}{\pi^k}\right]$.

Lemma 3.1. *A is a coalgebra.*

Proof. We show that units s and t satisfy conditions (a), (b) and (c) of Lemma 2.1. We have

$$\zeta_3^{-1}s^{-1} = 1 + \zeta_2\nu^{-1}\pi^{l+(q/2)}(1+\nu\pi^{-l/2}), \tag{9}$$

thus

$$\zeta_2^{-1}s^{-2} = G(u^2, w) + T,$$

where T is an element of R with $\mathrm{ord}(T) \geq (e'/2) + l + (q/2)$.

Moreover,

$$t^2 = s^2\left(\frac{1+w}{1-w}\right) - \frac{2(1+\pi^m)}{\zeta_2(1-w)} + N, \tag{10}$$

where N is an element of R with $\mathrm{ord}(N) \geq e' + l$.

Now

$$\begin{aligned}
\tilde{u}^{-2} - s^{-2}t^2 &= \tilde{u}^{-2} - \frac{1+w}{1-w} + \frac{2s^{-2}(1+\pi^m)}{\zeta_2(1-w)} - s^{-2}N \\
&= \frac{-2}{1-w}\left(\frac{-\tilde{u}^{-2}(1-w)}{2} + \frac{1+w}{2} - \zeta_2^{-1}s^{-2}(1+\pi^m)\right) - s^{-2}N \\
&= \frac{-2}{1-w}\left(G(u^2,w) - \zeta_2^{-1}s^{-2} - \zeta_2^{-1}s^{-2}\pi^m\right) - s^{-2}N \\
&= \frac{2}{1-w}\left(T + \zeta_2^{-1}s^{-2}\pi^m\right) - s^{-2}N \\
&= \frac{2T}{1-w} + \frac{2\zeta_2^{-1}s^{-2}\pi^m}{1-w} - s^{-2}N,
\end{aligned}$$

with

$$\begin{aligned}
\mathrm{ord}\left(\frac{2T}{1-w}\right) &\geq e' + \frac{e'}{2} + l + \frac{q}{2} - j' - \frac{k}{2} \\
&= e' + \frac{e'}{2} + i' + \frac{j}{2} + \frac{j'}{2} + \frac{k}{4} - j' - \frac{k}{2} \\
&= e' + j + i' - \frac{k}{4} \\
&\geq 2j + 2i' \quad (\text{since } i \geq 2j,)
\end{aligned}$$

$$\begin{aligned}\operatorname{ord}\left(\frac{2\zeta_2^{-1}s^{-2}\pi^m}{1-w}\right) &\geq e'+2i'+j+\frac{k}{2}-j'-\frac{k}{2}\\ &= 2j+2i',\end{aligned}$$

and

$$\begin{aligned}\operatorname{ord}(s^{-2}N) &\geq e'+l\\ &= e'+i'+\frac{j}{2}\\ &\geq 2j+2i' \quad (\text{since } i\geq 2j.)\end{aligned}$$

Hence $\operatorname{ord}(\tilde{u}^{-1}-s^{-1}t)\geq j+i'$.

Since $\operatorname{ord}(1-\tilde{u}^2)\geq 2j+i'$, $\operatorname{ord}(\tilde{u}-s^{-1}t)\geq j+i'$. Thus s and t satisfy condition (a) of Lemma 2.1.

Moreover, from (10),

$$t^2 = s^2\left(\frac{1+w}{1-w}\right)-\frac{2(1+\pi^m)}{\zeta_2(1-w)}+N, \quad \textit{or}$$

$$t^2\left(\frac{1-w}{2}\right) = s^2\left(\frac{1+w}{2}\right)-\frac{1+\pi^m}{\zeta_2}+\frac{(1-w)N}{2}, \quad \textit{or}$$

$$\zeta_2 s^2 G(-s^{-2}t^2,w)-1=\pi^m-\frac{\zeta_2 N(1-w)}{2},$$

with

$m\geq 2i'+j+(k/2)\geq 2i'+k$, and

$$\begin{aligned}\operatorname{ord}\left(\frac{\zeta_2 N(1-w)}{2}\right) &= e'+l+j'+\frac{k}{2}-e'\\ &= i'+\frac{j}{2}+j'+\frac{k}{2}\\ &\geq 2i'+k.\end{aligned}$$

Thus s,t satisfy condition (b) of Lemma 2.1.

Finally, from (9), one has $\operatorname{ord}(1-\zeta_3 s)=i'+(k/4)$, thus condition (c) of Lemma 2.1 is satisfied. Therefore A is a coalgebra.

□

Next put $B = A(k', j', \tilde{w}) \left[\dfrac{\gamma\beta - 1}{\pi^{i'}}\right]$, with

$$\beta = \sum_{r=0}^{3} v_r \iota_r = \iota_0 + \left(\frac{\tilde{u}y - x}{\zeta_3(y^2 - x^2)}\right)\iota_1 + \tilde{u}\iota_2 + \left(\frac{y - \tilde{u}x}{\zeta_3(y^2 - x^2)}\right)\iota_3,$$

where $y = \dfrac{u_1 - u_3}{2}$, $x = \dfrac{u_1 + u_3}{2}$.

If we now assume the additional conditions: $j' \geq 2i'$, $k' \geq 4i'$, $j \geq 4k$ and $e' \geq i + j + k$, then B is a coalgebra by Lemma 2.2, and A and B are dual Hopf orders by Theorem 2.5.

We claim that A is, in fact, a realizable Hopf order in KC_8. To prove this we shall use N. Byott's theorem from [2] which states that A is realizable if and only if $A^* = B$ is monogenic and local. We first prove a lemma.

Lemma 3.2. *The unit* $v_1 = \dfrac{\tilde{u}y - x}{\zeta_3(y^2 - x^2)}$ *satisfies*

$$ord(\zeta_2 v_1^2 - 1) = 2i' + \frac{k}{2}.$$

Proof. Put $q = \dfrac{v_1 - v_3}{2}$, and $r = \dfrac{v_1 + v_3}{2}$. Let $z = \sum_{m=0}^{3} z_m e_m$, where

$$z_0 = 1, \quad z_1 = \frac{wq - r}{\zeta_3(q^2 - r^2)}, \quad z_2 = w, \quad z_3 = \frac{q - wr}{\zeta_3(q^2 - r^2)}.$$

Then by [13, Theorem 4.8],

$$E = A(i, j, u)\left[\frac{gz - 1}{\pi^k}\right] = B^* = A,$$

and therefore E is a Hopf order.

From the necessary condition

$$\text{ord}\left(\langle(\overline{\gamma}a_{v_1^{-1}v_3} - 1) \otimes (\overline{\gamma}a_{v_1^{-1}v_3} - 1), \Delta(z) - z \otimes z\rangle\right) \geq 2i' + k,$$

one has

$$\text{ord}(\zeta_2 v_1^2 G(-v_1^{-2}v_3^2, w) - 1) \geq k + 2i'.$$

Since $\text{ord}(1 + v_1^{-2}v_3^2) = \text{ord}(1 - u^2)$,

$$\text{ord}(G(-v_1^{-2}v_3^2, w) - 1) = \text{ord}(G(u^2, w) - 1).$$

Therefore $\mathrm{ord}(G(-v_1^{-2}v_3^2, w) - 1) = 2i' + (k/2)$, since $\mathrm{ord}(1-u) = i' + (j/2)$ and $\mathrm{ord}(1-w) = j' + (k/2)$. It follows that $\mathrm{ord}(\zeta_2 v_1^2 - 1) = 2i' + (k/2)$. □

Theorem 3.3. *$B = A(k', j', \tilde{w})\left[\frac{\gamma\beta - 1}{\pi^{i'}}\right]$ is monogenic, and is generated by $\frac{\gamma\beta-1}{\pi^{i'}}$. Thus $A = A(i, j, u)\left[\frac{gb-1}{\pi^k}\right]$ is a realizable Hopf order in KC_8.*

Proof. We claim that $B = R\left[\frac{\gamma\beta - 1}{\pi^{i'}}\right]$. Clearly, $R\left[\frac{\gamma\beta - 1}{\pi^{i'}}\right] \subseteq B$. So it remains to show the reverse containment "$\supseteq$".

One has

$$R\left[\frac{\gamma^2\beta^2 - 1}{\pi^{2i'}}\right] \subseteq R\left[\frac{\gamma\beta - 1}{\pi^{i'}}\right], \tag{11}$$

and

$$R\left[\frac{\gamma^2\beta^2 - 1}{\pi^{2i'}}\right] \subseteq A(k', j', \tilde{w}). \tag{12}$$

We claim that

$$\mathrm{disc}\left(R\left[\frac{\gamma^2\beta^2 - 1}{\pi^{2i'}}\right]\right) = \mathrm{disc}\left(A(k', j', \tilde{w})\right),$$

so that equality holds in (12). To this end,

$$\begin{aligned}\mathrm{disc}\left(R\left[\frac{\gamma^2\beta^2 - 1}{\pi^{2i'}}\right]\right) &= \pi^{-24i'}\mathrm{disc}(1, \gamma^2\beta^2 - 1, (\gamma^2\beta^2-1)^2, (\gamma^2\beta^2-1)^3) \\ &= \pi^{-24i'}\mathrm{disc}(1, \gamma^2\beta^2, (\gamma^2\beta^2)^2, (\gamma^2\beta^2)^3).\end{aligned}$$

Now

$$\begin{pmatrix} 1 \\ \gamma^2\beta^2 \\ (\gamma^2\beta^2)^2 \\ (\gamma^2\beta^2)^3 \end{pmatrix} = M \begin{pmatrix} e_0 \\ e_1 \\ e_2 \\ e_3 \end{pmatrix},$$

where

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \zeta_2 v_1^2 & u^{-2} & \zeta_2^3 v_3^2 \\ 1 & (\zeta_2 v_1^2)^2 & (u^{-2})^2 & (\zeta_2^3 v_3^2)^2 \\ 1 & (\zeta_2 v_1^2)^3 & (u^{-2})^3 & (\zeta_2^3 v_3^2)^3 \end{pmatrix}.$$

Since $\mathrm{disc}(e_0, e_1, e_2, e_3) = R$, it suffices to compute $(det(M))^2$. Now,

$$\det(M) = (\zeta_2^3 v_3^2 - 1)(\zeta_2^3 v_3^2 - \zeta_2 v_1^2)(\zeta_2^3 v_3^2 - u^{-2})(u^{-2} - \zeta_2 v_1^2)(u^{-2} - 1)(\zeta_2 v_1^2 - 1).$$

We have

$$\begin{aligned} \zeta_2^3 v_3^2 - \zeta_2 v_1^2 &= \zeta_2^3 (v_3^2 + v_1^2) \\ &= -u_1^{-2} u_3^{-2} \left((y - \tilde{u}x)^2 + (\tilde{u}y - x)^2 \right) \\ &= -u_1^{-2} u_3^{-2} \left((x^2 + y^2)(\tilde{u}^2 + 1) - 4\tilde{u}xy \right), \end{aligned}$$

where $x^2 + y^2$ is a unit, $\mathrm{ord}(4\tilde{u}xy) = \mathrm{ord}(1 - w^2) = 2j' + k$, and $\mathrm{ord}(\tilde{u}^2 + 1) = \mathrm{ord}(1 - u^2) = 2i' + j$.

Since $2j' + k > 2i' + j$,

$$\mathrm{ord}(\zeta_2^3 v_3^2 - \zeta_2 v_1^2) = 2i' + j.$$

By Lemma 3.2, $\mathrm{ord}(1 - \zeta_2 v_1^2) = 2i' + (k/2)$, hence the relation $2i' + j > 2i' + (k/2)$ implies

$$\mathrm{ord}(1 - \zeta_2 v_1^2) = \mathrm{ord}(1 - \zeta_2^3 v_3^2) = 2i' + \frac{k}{2},$$

$$\mathrm{ord}(\zeta_2^3 v_3^2 - u^{-2}) = \mathrm{ord}(u^{-2} - \zeta_2 v_1^2) = 2i' + \frac{k}{2}.$$

It follows that

$$\begin{aligned} \mathrm{ord}(\det(M)) &= 2(2i' + j) + 4\left(2i' + \frac{k}{2}\right) \\ &= 12i' + 2j + 2k. \end{aligned}$$

Thus,

$$\mathrm{disc}\left(R\left[\frac{\gamma^2 \beta^2 - 1}{\pi^{2i'}} \right] \right) = 2(12i' + 2j + 2k) - 24i' = 4(j + k).$$

Meanwhile, one has $\mathrm{disc}(A(k', j', \tilde{w})) = 4(j + k)$, cf. [10, §1], so that equality holds in (12).

Now from (11),

$$A(k', j', \tilde{w}) \subseteq R\left[\frac{\gamma\beta - 1}{\pi^{i'}}\right],$$

and consequently, $B \subseteq R\left[\frac{\gamma\beta - 1}{\pi^{i'}}\right]$, which completes that proof that B is monogenic and A is realizable.

□

We give an example of a realizable Hopf order in KC_8.

Example 3.4. Let $e = e' = 100$, $i = 76$, $j = 16$, $k = 4$, then $\mathrm{ord}(\nu) = 50$, and

$$i = 76 \geq 2j = 2 \cdot 16 = 32;$$

$$j = 16 \geq 4k = 4 \cdot 4 = 16;$$

$$j' = 84 \geq 2i' = 2 \cdot 24 = 48;$$

$$k' = 96 \geq 4i' = 4 \cdot 24 = 96;$$

$$e' = 100 \geq i + j + k = 76 + 16 + 4 = 96;$$

$$m = 2i' + j + (k/2) = 2 \cdot 24 + 16 + 2 = 66.$$

We have $q = 84 + 2 = 86$ and $l = 24 + 8 = 32$. Set $u = 1 + \pi^l = 1 + \pi^{32}$ and $w = 1 + \pi^q = 1 + \pi^{86}$. Then

$$s = \zeta_3^{-1}\left(1 + \zeta_2\nu^{-1}\pi^{75}(1 + \nu\pi^{-16})\right)^{-1},$$

$$t = \zeta_2\pi^{-43}\left(s(\nu + \pi^{43}) + \zeta_2\zeta_3^{-1}\nu(1 + \pi^{33})\right),$$

One has the dual Hopf orders,

$$A = A(76, 16, u)\left[\frac{gb-1}{\pi^4}\right] \quad \text{and} \quad A^* = B = A(96, 84, \tilde{w})\left[\frac{\gamma\beta-1}{\pi^{24}}\right],$$

with

$$b = \sum_{r=0}^{3} u_r e_r = e_0 + \left(\frac{wd-c}{\zeta_3(d^2-c^2)}\right)e_1 + we_2 + \left(\frac{d-wc}{\zeta_3(d^2-c^2)}\right)e_3,$$

$$d = \frac{s-t}{2}, \quad c = \frac{s+t}{2},$$

$$\beta = \sum_{r=0}^{3} v_r \iota_r = \iota_0 + \left(\frac{\tilde{u}y-x}{\zeta_3(y^2-x^2)}\right)\iota_1 + \tilde{u}\iota_2 + \left(\frac{y-\tilde{u}x}{\zeta_3(y^2-x^2)}\right)\iota_3,$$

$$y = \frac{u_1-u_3}{2}, \quad x = \frac{u_1+u_3}{2}.$$

The Hopf order A is realizable and the Hopf order $B = A^*$ is monogenic.

A natural question arises: Is the realizable Hopf order A distinct from all of the known realizable Hopf orders in KC_8?

Theorem 3.5. *The realizable Hopf order A of Example 3.4 is distinct from all known realizable Hopf orders in KC_8.*

Proof. Underwood and Childs [13] have identified various types of Hopf orders in KC_{p^3}: *cohomological*, *ILD*, *duality* and *formal group*. For $p \geq 2$, no ILD Hopf order which is not cohomological is realizable [13, Theorem 5.2]. Likewise, for $p \geq 2$, no duality Hopf order is realizable [13, Theorem 5.3]. For $p > 2$, no formal group Hopf order is realizable [13, Theorem 5.4]. The case $p = 2$ was not considered in [13, Theorem 5.4]. But, using the methods of this paper one can show that formal group Hopf orders in KC_8 have triangular duals which are not monogenic. Thus there are no realizable formal group Hopf orders for $p \geq 2$.

It follows that the known realizable Hopf orders in KC_8 are either cohomological, that is, of the form given in [12, Theorem 3.3.1], or are of the form given in [13, Theorem 5.7]. In both cases, these Hopf orders are extended from dual Larson orders in KC_4. In the Hopf order A of Example 3.4, however, the

Hopf order $A(76, 16, u)$ is not dual Larson. Thus A cannot be of the known forms. □

Remark 3.6. The Hopf order A from Example 3.4 is not *triangular* in the sense of [13, §1], while B is triangular.

Remark 3.7. The Hopf order A of Example 3.4 satisfies the *valuative condition for n=3*, cf. [11, §4.0], [13, §3].

REFERENCES

[1] N. Byott, Cleft extensions of Hopf algebras, *Proc. London Math. Soc.*, **67**, (1993), 227-307.

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

[3] L. N. Childs, Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory, American Mathematical Society, Mathematical Surveys and Monographs **80**, 2000.

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

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

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

[7] R. G. Larson, Hopf algebra orders determined by group valuations, *J. Algebra*, **38**, (1976), 414-452.

[8] S. Montgomery, Hopf Algebras and Their Actions on Rings, American Mathematical Society, CBMS Regional Conference Series in Mathematics, 82, (1993).

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

[10] R. Underwood, R-Hopf algebra orders in KC_{p^2}, *J. Algebra*, **169**, (1994), 418-440.

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

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

[13] R. Underwood, L. N. Childs, Duality for Hopf orders, *Trans. Amer. Math. Soc.*, to appear (posted online April 22, 2005.)

Received: September 25, 2005