Hopf Orders in KC_{p^3}

Robert G. Underwood
Department of Mathematics and Computer Science
Auburn University at Montgomery
Montgomery, Alabama

June 13, 2019

1. Introduction

Let p be a prime number and let $n \geq 1$. Let K be a finite extension of the p-adic rationals $\mathbb{Q}_p$ containing ζ_n, a primitive p^nth root of unity with $\zeta_n^p = \zeta_{n-1}$. Let $\nu(a)$ be the valuation of a in K normalized so that $\nu(\pi) = 1$ where π is a parameter of K.

Let R denote the ring of integers of K and let $\nu(p) = e$ denote the ramification index of p in R. Put $e' = e/(p-1)$.

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 $\langle\ ,\ \rangle$.

The group algebra KC_{p^n} is a K-Hopf algebra where the comultiplication $\Delta : KC_{p^n} \to KC_{p^n} \otimes KC_{p^n}$, counit $\varepsilon : KC_{p^n} \to K$, and coinverse $\sigma : KC_{p^n} \to KC_{p^n}$ maps are defined by $g \mapsto g \otimes g$, $g \mapsto 1$, and $g \mapsto g^{-1}$, respectively.

An R-**order in** KC_{p^n} is a subring H of KC_{p^n} which is a finitely generated R-module and which satisfies $H \otimes_R K \cong KC_{p^n}$. The R-order H is an R-**Hopf order in** KC_{p^n} if $\Delta(H) \subseteq H \otimes H$.

The invariance of H under Δ implies that $\varepsilon(H) \subseteq R$ and $\sigma(H) \subseteq H$, hence Δ, ϵ, and σ give H the structure of a Hopf algebra over R. The integral group ring RC_{p^n} is an easy example of an R-Hopf order in KC_{p^n}.

The classification of Hopf orders in KC_{p^n} is complete for the cases $n = 1, 2$. This is due to the work of various authors: J. Tate and F. Oort [TO70], R. Larson [La76], C. Greither [Gr92], N. Byott [By93], U. [Un94], and U. and L. Childs [UC06].

The classification for $n > 2$ is an open problem however.

In the case $n = 3$, large classes of Hopf orders have been constructed: U. and L. Childs have identified collections of **triangular**, **cohomological**, **ILD**, **duality** and **formal group** Hopf orders, see [Un96], [CU03], and [UC06].

Nevertheless, a complete classification remains elusive. We shall consider the case $n = 3$ in this paper, recalling results found in [Un08]. We begin with a review of the case $n = 2$.

2. The $n = 2$ case

Let $\overline{g}$ denote the image of g under the mapping $KC_{p^2} \to KC_p$, $g^p \mapsto 1$; let $\overline{\gamma}$ denote the image of γ under the mapping $K\hat{C}_{p^2} \to K\hat{C}_p$, $\gamma^p \mapsto 1$. For an integer m, $0 \leq m \leq e'$, set $m' = e' - m$.

Let $i, j \geq 0$ be integers with $e' \geq i, j$. Then

$$H(i) = R\left[\frac{g^p - 1}{\pi^i}\right] \quad \text{and} \quad H(j) = R\left[\frac{\overline{g} - 1}{\pi^j}\right]$$

are Hopf orders in KC_p [Ch00, §31].

It is well-known that all Hopf orders in KC_p are of the form given above (see [Ch00, 31.13].)

The linear duals of these Hopf orders are Hopf orders in $K\hat{C}_p \cong KC_p$ of the form

$$H(i)^* = H(i') = R\left[\frac{\overline{\gamma}-1}{\pi^{i'}}\right] \quad \text{and} \quad H(j)^* = H(j') = R\left[\frac{\gamma^p-1}{\pi^{j'}}\right].$$

We extend the rank p Hopf order $H(i)$ to obtain a Hopf order in KC_{p^2}

This has always come down to selecting the "correct" element $\frac{gb-1}{\pi^j} \in KC_{p^2}$ which maps to $\frac{\overline{g}-1}{\pi^j}$ under the canonical surjection $KC_{p^2} \to KC_p$.

For $m = 0, \ldots, p-1$, let

$$\iota_m = \frac{1}{p} \sum_{a=0}^{p-1} \zeta_1^{-ma} \gamma^{pa},$$

$$e_m = \frac{1}{p} \sum_{a=0}^{p-1} \zeta_1^{-ma} g^{pa},$$

denote the minimal idempotents for $K\langle \gamma^p \rangle \cong KC_p$, and $K\langle g^p \rangle \cong KC_p$, respectively.

Let $s_0 = 1$, and s_m, $m = 1, \ldots, p-1$, be units of R and set

$$\tau = \sum_{m=0}^{p-1} s_m \iota_m, \quad \tau \in K\langle \gamma^p \rangle;$$

Let $x_0 = 1$, and x_m, $m = 1, \ldots, p-1$, be indeterminates and set

$$x = \sum_{m=0}^{p-1} x_m e_m, \quad x \in K\langle g^p \rangle.$$

We seek values for x_m, $m > 0$, so that

$$\langle (\gamma^p - 1)^q (\gamma\tau - 1)^r, gx - 1 \rangle_2 = 0, \tag{1}$$

for $q, r = 0, \ldots, p-1$, $r > 0$.

Proposition 2.1. *The solution to (1) is* $x_m = \zeta_2^{-m} s_1^{-m}$ *for* $m = 0, \ldots, p-1$. *Thus*

$$\langle (\gamma^p - 1)^q (\gamma\tau - 1)^r, gb - 1 \rangle_2 = 0, \tag{2}$$

for $q, r = 0, \ldots, p-1$, $r > 0$, *where*

$$b = \sum_{m=0}^{p-1} \zeta_2^{-m} s_1^{-m} e_m \quad \in K\langle g^p \rangle.$$

Proof. Direct calculation. □

Put $\tilde{s}_1 = \zeta_2^{-1} s_1^{-1}$. Then b is the familiar "Greither" quantity $a_{\tilde{s}_1}$, which we shall write as $G(g^p, \tilde{s}_1)$, where

$$G(x, y) = \frac{1}{p} \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} \zeta_1^{-mn} x^m y^n$$

denotes the Gauss sum.

Now let $j > 0$ be an integer with $i \geq j/p$. Let

$$A(i, j, \tilde{s}_1) = H(i) \left[\frac{gG(g^p, \tilde{s}_1) - 1}{\pi^j} \right]$$

denote the R-module which is the $H(i)$-span of the set

$$\left\{ 1, \frac{gG(g^p, \tilde{s}_1) - 1}{\pi^j}, \left(\frac{gG(g^p, \tilde{s}_1) - 1}{\pi^j} \right)^2, \right.$$

$$\left. \ldots, \left(\frac{gG(g^p, \tilde{s}_1) - 1}{\pi^j} \right)^{p-1} \right\}.$$

Proposition 2.2. *Assume that* $\nu(\zeta_1 s_1^p - 1) \geq pi' + j$. *Then* $A(i, j, \tilde{s}_1)$ *is a subcoalgebra of* KC_{p^2}.

Proof. Since $A(i, j, \tilde{s}_1) \subseteq KC_{p^2}$, the counit map ε of KC_{p^2} restricts to give counit map $\varepsilon : A(i, j, \tilde{s}_1) \to R$.

From $i \geq j/p$, we see that $\nu(\zeta_1 s_1^p - 1) \geq pi' + j$ implies $\nu(\zeta_2 s_1 - 1) \geq i' + j/p$. Thus by [Ch00, (31.8)],

$$G(g^p, \tilde{s}_1) \in 1 + \pi^{j/p} H(i),$$

and so, $G(g^p, \tilde{s}_1)$ is a unit in $H(i)$. The result then follows from [Ch00, (31.2), (31.10)]. $\square$

Next, let $y_0 = 1$, and y_m, $m = 1, \ldots, p-1$, be indeterminates and set

$$y = \sum_{m=0}^{p-1} x_m \iota_m, \quad x \in K\langle \gamma^p \rangle.$$

We seek values for y_m, $m > 0$, so that

$$\langle \gamma y - 1, (g^p - 1)^q (gG(g^p, \tilde{s}_1) - 1)^r \rangle_2 = 0, \tag{3}$$

for $q, r = 0, \ldots, p-1$, $r > 0$.

By Proposition 2.1, the solution to (3) is $y_m = s_1^m$, for $m = 0, \ldots, p-1$. Thus $y = G(\gamma^p, s_1)$.

Now assume that $i \geq pj$, and $e' \geq i + j$. Let

$$A(j', i', s_1) = H(j') \left[\frac{\gamma G(\gamma^p, s_1) - 1}{\pi^{i'}} \right]$$

denote the R-module which is the $H(j')$-span of the set

$$\left\{ 1, \frac{\gamma G(\gamma^p, s_1) - 1}{\pi^{i'}}, \left(\frac{\gamma G(\gamma^p, s_1) - 1}{\pi^{i'}} \right)^2, \right.$$

$$\left. \ldots, \left(\frac{\gamma G(\gamma^p, s_1) - 1}{\pi^{i'}} \right)^{p-1} \right\}.$$

Proposition 2.3. *Assume that $i \geq pj$, $e' \geq i + j$, and $\nu(\zeta_1 s_1^p - 1) \geq pi' + j$. Then $A(j', i', s_1)$ is a subcoalgebra of $K\hat{C}_{p^2}$.*

Proof. Since $A(j', i', s_1) \subseteq K\hat{C}_{p^2}$, the counit map ε of $K\hat{C}_{p^2}$ restricts to give counit map $\varepsilon : A(j', i', s_1) \to R$.

Since $e' \geq i + j$, $\nu(\zeta_1 s_1^p - 1) \geq pi' + j$ implies $\nu(\zeta_1 s_1^p - 1) \geq pj + i'$. Since $i \geq pj$, $\nu(\zeta_1 s_1^p - 1) \geq pj + i'$ yields $\nu(s_1^p - 1) \geq pj + i'$. Thus $G(\gamma^p, s_1)$ is a unit in $H(j')$. Note that $i \geq pj$ implies $j' \geq i'/p$. The result then follows from [Ch00, (31.2), (31.10)]. $\square$

To summarize: for $i \geq pj$, $e' \geq i + j$, $\nu(\zeta_1 s_1^p - 1) \geq pi' + j$, we have that

$$A(i, j, \tilde{s}_1) = R\left[\frac{g^p - 1}{\pi^i}, \frac{gG(g^p, \tilde{s}_1) - 1}{\pi^j}\right]$$

is a subcoalgebra of KC_{p^2}, and

$$A(j', i', s_1) = R\left[\frac{\gamma^p - 1}{\pi^{j'}}, \frac{\gamma G(\gamma^p, s_1) - 1}{\pi^{i'}}\right]$$

is a subcoalgebra of $K\hat{C}_{p^2}$.

Proposition 2.4. *Suppose that $i \geq pj$, $e' \geq i + j$, and $\nu(\zeta_1 s_1^p - 1) \geq pi' + j$. Then*

$$A(i, j, \tilde{s}_1) = R\left[\frac{g^p - 1}{\pi^i}, \frac{gG(g^p, \tilde{s}_1) - 1}{\pi^j}\right]$$

is an R-Hopf order in KC_{p^2} with linear dual

$$A(j', i', s_1) = R\left[\frac{\gamma^p - 1}{\pi^{j'}}, \frac{\gamma G(\gamma^p, s_1) - 1}{\pi^{i'}}\right]$$

in $K\hat{C}_{p^2}$.

Proof. We show that $A(j', i', s_1)$ is a Hopf order in $K\hat{C}_{p^2}$. First note that $A(i, j, \tilde{s}_1)^*$ is an algebra. From $A(i, j, \tilde{s}_1)^* \cap K\hat{C}_p = H(j')$ and (3), we have $A(j', i', s_1) \subseteq A(i, j, \tilde{s}_1)^*$. Moreover, $\frac{\gamma G(\gamma^p, s_1)-1}{\pi^{i'}}$ satisfies a monic polynomial of degree p with coefficients in $H(j')$. Thus $A(j', i', s_1)$ is an algebra as well as a coalgebra.

The coinverse map of $A(j', i', s_1)$ can now be defined as the composite σ of the iterated comultiplication and multiplication maps

$$A(j', i', s_1) \to \bigotimes^{p^2-1} A(j', i', s_1) \to A(j', i', s_1).$$

Hence, $A(j', i', s_1)$ is an R-Hopf order in $K\hat{C}_{p^2}$.

A similar argument shows that $A(i, j, \tilde{s}_1)$ is an R-Hopf order in KC_{p^2}. A discriminant argument then shows that $A(j', i', s_1) = A(i, j, \tilde{s}_1)^*$. □

3. The $n = 3$ case

Let $\overline{g}$ denote the image of g under the mapping $KC_{p^3} \to KC_{p^2}$, $g^{p^2} \mapsto 1$; let $\overline{\gamma}$ denote the image of γ under the mapping $K\hat{C}_{p^3} \to K\hat{C}_{p^2}$, $\gamma^{p^2} \mapsto 1$.

Let

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

and

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

be Hopf orders in KC_{p^2} [Ch00, §31].

By [Un94, Theorem 1.3.1], $i \geq j \geq k$. Moreover, $e' \geq i$, $\mathrm{ord}(1-u) \geq i' + (j/p)$ and $\mathrm{ord}(1-w) \geq j' + (k/p)$. We assume that $j' > pi'$, $j + i' > \mathrm{ord}(1-\tilde{u})$ and $j' + k > \mathrm{ord}(1-w)$.

The linear duals of these Hopf orders are Hopf orders in $K\hat{C}_{p^2}$ of the form

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

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

[UC06, Theorem 1.2].

Let

$$\iota_{pm+n} = \frac{1}{p^2} \sum_{a=0}^{p-1} \sum_{b=0}^{p-1} \zeta_2^{-(pm+n)(pa+b)} \gamma^{p(pa+b)},$$

$$\rho_q = \frac{1}{p} \sum_{n=0}^{p-1} \zeta_1^{-qn} \overline{\gamma}^{pn},$$

$$e_{pm+n} = \frac{1}{p^2} \sum_{a=0}^{p-1} \sum_{b=0}^{p-1} \zeta_2^{-(pm+n)(pa+b)} g^{p(pa+b)}, \quad \text{and}$$

$$f_q = \frac{1}{p} \sum_{n=0}^{p-1} \zeta_1^{-qn} \overline{g}^{pn},$$

$m, n = 0, \ldots, p-1$, $0 \leq q \leq p-1$, denote the minimal idempotents for $K\langle \gamma^p \rangle \cong K\hat{C}_{p^2}$, $K\langle \overline{\gamma}^p \rangle \cong K\hat{C}_p$, $K\langle g^p \rangle \cong KC_{p^2}$, and $K\langle \overline{g}^p \rangle \cong KC_p$, respectively.

Let s_{pm+n}, $m, n = 0, \ldots, p-1$, be units of R with $s_{pm} = \tilde{u}^m$, and set

$$\tau = \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} s_{pm+n} \iota_{pm+n}, \quad \tau \in K\langle \gamma^p \rangle;$$

$$d = \sum_{q=0}^{p-1} s_1^{-1} s_{pq+1} \rho_q, \quad d \in K\langle \overline{\gamma}^p \rangle.$$

Let x_{pm+n}, $m, n = 0, \ldots, p-1$, be indeterminates with $x_{pm} = w^m$, and set

$$x = \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} x_{pm+n} e_{pm+n}, \quad x \in K\langle g^p \rangle.$$

We seek values for x_{pm+n}, $n > 0$, so that

$$\left\langle (\gamma^{p^2} - 1)^q (\gamma^p G(\gamma^{p^2}, \tilde{w}) - 1)^r (\gamma\tau - 1)^s, gx - 1 \right\rangle_3 = 0, \qquad (4)$$

for $q, r, s = 0, \ldots, p-1$, $r + s > 0$.

Proposition 3.1 *The solution to (4) is*

$$x_{pm+n} = \zeta_3^{-n} s_1^{-n} \langle \overline{\gamma}^{pm} d^{-n}, G(\overline{g}^p, w) \rangle_1,$$

for $m, n = 0, \ldots, p-1$. *Thus*

$$\left\langle (\gamma^{p^2} - 1)^q (\gamma^p G(\gamma^{p^2}, \tilde{w}) - 1)^r (\gamma\tau - 1)^s, gb - 1 \right\rangle_3 = 0, \qquad (5)$$

for $q, r, s = 0, \ldots, p-1$, $r + s > 0$, *when*

$$b = \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} \zeta_3^{-n} s_1^{-n} \langle \overline{\gamma}^{pm} d^{-n}, G(\overline{g}^p, w) \rangle_1 e_{pm+n}.$$

Proof. See [Un08]. □.

In the special case that

$$\tau = \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} \tilde{u}^m s^n \iota_{pm+n},$$

for s a unit of R, the solution to (4) is

$$\begin{aligned} x_{pm+n} &= \zeta_3^{-n} s^{-n} \langle \overline{\gamma}^{pm} G(\overline{\gamma}^p, \tilde{u})^{-n}, G(\overline{g}^p, w) \rangle_1 \\ &= \zeta_3^{-n} s^{-n} \langle G(\overline{\gamma}^p, \zeta_1^m \tilde{u}^{-n}), G(\overline{g}^p, w) \rangle_1 \\ &= \zeta_3^{-n} s^{-n} G(\zeta_1^m \tilde{u}^{-n}, w). \end{aligned}$$

for $m, n = 0, \ldots, p-1$. Thus if

$$b = \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} \zeta_3^{-n} s^{-n} G(\zeta_1^m \tilde{u}^{-n}, w) e_{pm+n},$$

then

$$\left\langle (\gamma^{p^2} - 1)^q (\gamma^p G(\gamma^{p^2}, \tilde{w}) - 1)^r (\gamma\tau - 1)^s, gb - 1 \right\rangle_3 = 0, \qquad (6)$$

for $q, r, s = 0, \ldots, p-1$, $r + s > 0$.

Now let

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

denote the R-module which is the $A(i,j,u)$-span of the set

$$\left\{1, \frac{gb-1}{\pi^k}, \left(\frac{gb-1}{\pi^k}\right)^2, \ldots, \left(\frac{gb-1}{\pi^k}\right)^{p-1}\right\}.$$

Proposition 3.2. *Suppose that* $j' > pi'$ *and* $\nu(\zeta_2 s^p - G(u^p, w)) \geq pi' + k$. *Then* H *is a subcoalgebra of* KC_{p^3}.

Proof. See [Un08].

□

Let y_{pm+n}, $m, n = 0, \ldots, p-1$ be indeterminates and set

$$y = \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} y_{pm+n} \iota_{pm+n}, \quad y_{pm} = \tilde{u}^m.$$

The y_{pm+n} are the analogs in the dual situation for x_{pm+n}. Then, following the construction of b as in the previous text, we find values for y_{pm+n}, $n > 0$, for which

$$\left\langle \gamma y - 1, (g^{p^2} - 1)^l (g^p G(g^{p^2}, u) - 1)^m (gb - 1)^t \right\rangle_3 = 0, \qquad (7)$$

for $l, m, t = 0, \ldots, p-1$, $m + t > 0$.

$$\begin{aligned} y_{pm+n} &= \zeta_3^{-n} \sum_{l=0}^{p-1} \phi_{m,l}^{(n)} \tilde{u}^l \\ &= \zeta_3^{-n} u_1^{-n} \langle \overline{g}^{pm} c^{-n}, a_{\tilde{u}} \rangle, \end{aligned}$$

for $m, n = 0, \ldots, p-1$, $n > 0$. The computation of y_{pm+n} is analogous to the computation of x_{pm+n}.
Thus if

$$y = \beta = \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} y_{pm+n} \iota_{pm+n}, \quad y_{pm} = \tilde{u}^m,$$

then (7) is satisfied.

Let $J = A(k', j', \tilde{w}) \left[\frac{\gamma\beta - 1}{\pi^{i'}} \right]$ denote the R-module which is the $A(k', j', \tilde{w})$-span of the set

$$\left\{ 1, \frac{\gamma\beta - 1}{\pi^{i'}}, \left(\frac{\gamma\beta - 1}{\pi^{i'}} \right)^2, \ldots, \left(\frac{\gamma\beta - 1}{\pi^{i'}} \right)^{p-1} \right\}.$$

Proposition 3.3. *Suppose H is an R-coalgebra as constructed by Proposition 3.2. Suppose $i \geq pj$, $k' \geq p^2 i'$, $j \geq p^2 k > pk$, and $e' \geq i + j + k$. Then the R-module J is an R-coalgebra.*

Proof. See [Un08].

Proposition 3.4. *Suppose* $j' > pi'$, $i \geq pj$, $k' \geq p^2 i'$, $j \geq p^2 k > pk$, $e' \geq i + j + k$, *and* $\nu(\zeta_2 s^p - G(u^p, w)) \geq pi' + k$. *The coalgebras* $H = A(i, j, u)\left[\dfrac{gb-1}{\pi^k}\right]$ *and* $J = A(k', j', \tilde{w})\left[\dfrac{\gamma\beta - 1}{\pi^{i'}}\right]$ *are dual Hopf orders in* KC_{p^3}.

Proof. (Analogous to the $n = 2$ case.) We first show that the coalgebra J is a Hopf order. Since H^* is an algebra with $H^* \cap K\hat{C}_{p^2} = A(k', j', \tilde{w})$, $\dfrac{\gamma\beta - 1}{\pi^{i'}} \in H^*$ satisfies a monic polynomial of degree p with coefficients in $A(k', j', \tilde{w})$. Thus J is an algebra as well as a coalgebra. The coinverse map of J can now be defined as the composite σ of the iterated comultiplication and multiplication maps $J \to \bigotimes^{p^3-1} J \to J$. Hence, J is an R-Hopf order in KC_{p^3}.
Observe that $J \subseteq H^*$ implies $H \subseteq J^*$. Since $J^* \cap KC_{p^2} = A(i, j, u)$, $\dfrac{gb - 1}{\pi^k}$ satisfies a monic polynomial of degree p with coefficients in $A(i, j, u)$. Thus H is a Hopf order. A well-known discriminant argument then shows that $H^* = J$.

□

Question: when is b trivial? That is, under what conditions do we have

$$b - 1 \in \pi^k A(i, j, u),$$

and hence

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

4. A Realizable Subclass

By [UC05, Proposition 2.3],

$$\begin{aligned}\nu(G(u^p, w) - 1) &= \nu(u^p - 1) + \nu(w - 1) - e' \\ &\geq pi' + j + j' + k/p - e' \\ &= pi' + k/p,\end{aligned}$$

and so, $\nu(\zeta_2 s^p - 1) \geq pi' + k/p$, hence, $\nu(\zeta_3 s - 1) \geq i' + k/p^2$.

Proposition 4.1. *Suppose $p \mid j$, $p^2 \mid k$, $\nu(1-u) = i' + j/p$, $\nu(1-w) = j' + k/p$, and $\nu(\zeta_3 s - 1) = i' + k/p^2$. Then the Hopf order $H = A(i,j,u)\left[\frac{gb-1}{\pi^k}\right] \subseteq KC_{p^3}$ is realizable in the sense that there exists a Galois extension L/K with group C_{p^3} for which $\mathcal{O}_L$ is an H-Galois algebra.*

Proof. See [Un08, §3]. □

5. A Revision and a Suggestion

Under the conditions given in Section 3, there exists a Hopf order in KC_{p^3} of the form

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

with

$$b = \sum_{m=0}^{p-1}\sum_{n=0}^{p-1} \zeta_3^{-n} s^{-n} G(\zeta_1^m \tilde{u}^{-n}, w) e_{pm+n}.$$

We claim that

$$b = G(G(g^{p^2},u)g^p, w)G(g^{p^2}, \zeta_3^{-1}s^{-1}).$$

To this end we compute the image of

$$G(G(g^{p^2}, u)g^p, w)G(g^{p^2}, \zeta_3^{-1}s^{-1})$$

under the isomorphism $KC_{p^2} \to \sum_{m=0}^{p-1}\sum_{n=0}^{p-1} Ke_{pm+n}$, $g^p \mapsto \sum_{m=0}^{p-1}\sum_{n=0}^{p-1} \zeta_2^{pm+n} e_{pm+n}$.

We obtain

$$
\begin{aligned}
& \sum_{m=0}^{p-1}\sum_{n=0}^{p-1} G(G((\zeta_2^{pm+n})^p,u)\zeta_2^{pm+n},w)G((\zeta_2^{pm+n})^p,\zeta_3^{-1}s^{-1})e_{pm+n} \\
= & \sum_{m=0}^{p-1}\sum_{n=0}^{p-1} G(G(\zeta_1^n,u)\zeta_1^m\zeta_2^n,w)G(\zeta_1^n,\zeta_3^{-1}s^{-1})e_{pm+n} \\
= & \sum_{m=0}^{p-1}\sum_{n=0}^{p-1} G(\zeta_1^m u^n\zeta_2^n,w)\zeta_3^{-n}s^{-n}e_{pm+n} \\
= & \sum_{m=0}^{p-1}\sum_{n=0}^{p-1} \zeta_3^{-n}s^{-n}G(\zeta_1^m\tilde{u}^{-n},w)e_{pm+n} \\
= & \ b.
\end{aligned}
$$

Thus the Hopf order is

$$R\left[\frac{g^{p^2}-1}{\pi^i}, \frac{g^p G(g^{p^2},u)-1}{\pi^j}, \frac{gG(g^{p^2},\zeta_3^{-1}s^{-1})G(g^p G(g^{p^2},u),w)-1}{\pi^k}\right].$$

Inspired by G. G. Elder, this suggests an inductive definition of Hopf orders in KC_{p^n}.

For r, $1 \leq r \leq n$, let

$$\Psi_r = g^{p^{n-r}} G(\Psi_1, u_{r,1}) G(\Psi_2, u_{r,2}) \cdots G(\Psi_{r-1}, u_{r,r-1}).$$

Then

$$R\left[\frac{\Psi_1 - 1}{\pi^{i_1}}, \frac{\Psi_2 - 1}{\pi^{i_2}}, \ldots \frac{\Psi_n - 1}{\pi^{i_n}}\right]$$

should be an R-Hopf order in KC_{p^n}.

When $n = 3$, $u_{2,1} = u$, $u_{3,1} = \zeta_3^{-1} s^{-1}$, $u_{3,2} = w$, $i_1 = i$, $i_2 = j$, $i_3 = k$, we have

$$\Psi_1 = g^{p^2}$$

$$\Psi_2 = g^p G(\Psi_1, u_{2,1}) = g^p G(g^{p^2}, u).$$

$$\Psi_3 = gG(\Psi_1, u_{3,1})G(\Psi_2, u_{3,2}) = gG(g^{p^2}, \zeta_3^{-1} s^{-1})G(g^p G(g^{p^2}, u), w).$$

And we recover the Hopf order

$$R\left[\frac{g^{p^2} - 1}{\pi^i}, \frac{g^p G(g^{p^2}, u) - 1}{\pi^j}, \frac{gG(g^{p^2}, \zeta_3^{-1} s^{-1})G(g^p G(g^{p^2}, u), w) - 1}{\pi^k}\right].$$

6. A Comparison with Byott and Elder

Recently, N. P. Byott and G. G. Elder have constructed a class of realizable Hopf orders in KC_p^3 [BE18, §5.3].

These Hopf orders have the form

$$R\left[\frac{\sigma_3-1}{\pi^{M_3}}, \frac{\sigma_2\sigma_3^{[-\mu_{2,3}]}-1}{\pi^{M_2}}, \frac{\sigma_1\sigma_3^{[-\mu_{1,3}]}\left(\sigma_2\sigma_3^{[-\mu_{2,3}]}\right)^{[-\mu_{1,2}]}-1}{\pi^{M_1}}\right]$$

where $C_p^3 = \langle \sigma_3, \sigma_2, \sigma_1 \rangle$, and where M_1, M_2, M_3 are integers, $\mu_{1,2}$, $\mu_{1,3}, \mu_{2,3}$ are elements of K satisfying certain conditions, and

$$X^{[Y]} = \sum_{m=0}^{p-1} \binom{Y}{m} (X-1)^m$$

is the truncated exponential.

The parameters $\mu_{a,b}$ satisfy the conditions

$$\nu(\mu_{2,3}) = \frac{M_2}{p} - M_3, \quad \nu(\mu_{1,3}) = \frac{M_1}{p^2} - M_3, \quad \nu(\mu_{1,2}) = \frac{M_1}{p} - M_2.$$

We compare the "Gauss sum" Hopf orders in KC_{p^3} with these "truncated exponential" Hopf orders in KC_p^3:

$$R\left[\frac{g^{p^2}-1}{\pi^i}, \frac{g^p G(g^{p^2},u)-1}{\pi^j}, \frac{gG(g^{p^2},\zeta_3^{-1}s^{-1})G(g^pG(g^{p^2},u),w)-1}{\pi^k}\right]$$

$$\Downarrow \quad \Uparrow$$

$$R\left[\frac{\sigma_3-1}{\pi^{M_3}}, \frac{\sigma_2\sigma_3^{[-\mu_{2,3}]}-1}{\pi^{M_2}}, \frac{\sigma_1\sigma_3^{[-\mu_{1,3}]}\left(\sigma_2\sigma_3^{[-\mu_{2,3}]}\right)^{[-\mu_{1,2}]}-1}{\pi^{M_1}}\right]$$

Clearly,

$$i \Longleftrightarrow M_3,\ j \Longleftrightarrow M_2,\ k \Longleftrightarrow M_1,$$

$$g^{p^2} \Longleftrightarrow \sigma_3,\ g^p \Longleftrightarrow \sigma_2,\ g \Longleftrightarrow \sigma_1.$$

But we also guess that

$$u \Longleftrightarrow -\mu_{2,3},$$

$$\zeta_3^{-1} s^{-1} \Longleftrightarrow -\mu_{1,3},$$

$$w \Longleftrightarrow -\mu_{1,2},$$

$$G(g^{p^2}, u) \Longleftrightarrow \sigma_3^{[-\mu_{2,3}]},$$

$$G(g^{p^2}, \zeta_3^{-1} s^{-1}) \Longleftrightarrow \sigma_3^{[-\mu_{1,3}]},$$

$$G(g^p G(g^{p^2}, u), w) \Longleftrightarrow (\sigma_2 \sigma_3^{[-\mu_{2,3}]})^{[-\mu_{1,2}]}.$$

Here is some evidence to support these assertions.

Let C_{p^2} denote the cyclic group of order p^2 generated by g. Let $i \geq j$ be integers with $e' \geq i + j$. Let v be a unit in R with $\nu(1 - v^p) \geq pi' + j$. Then

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

is an R-Hopf order in KC_{p^2}.

Let

$$\mu = \frac{1}{\zeta_1 - 1} \sum_{m=1}^{p-1} \frac{(1 - v)^m}{m}.$$

Proposition 6.1.([Un11], [El11], [El12]) *The Gauss sum Hopf order is a truncated exponential Hopf order, that is,*

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

Proof. We show that

$$\frac{G(g^p,v)-(g^p)^{[-\mu]}}{\pi^j} \in H(i).$$

□

Note that

$$\begin{aligned}\nu(1-v^p) &= p\nu(1-v)\\ &= p(\nu(\mu)+e')\\ &= \nu(\wp(\mu))+pe'.\end{aligned}$$

So, the condition $\nu(1-v^p) \geq pi'+j$ implies that $\nu(\wp(\mu)) \geq j-pi$. (Here $\wp(x) = x^p - x$.)

We *should* be able to convert the Gauss sum Hopf order in KC_{p^3} to a trunexp Hopf order in KC_{p^3}.

Recall that $\nu(\zeta_2 s^p - G(u^p, w)) \geq pi' + k$ is a sufficient condition for the existence of a Gauss sum Hopf order in KC_{p^3}:

$$R\left[\frac{g^{p^2}-1}{\pi^i}, \frac{g^p G(g^{p^2}, u)-1}{\pi^j}, \frac{gG(g^{p^2}, \zeta_3^{-1}s^{-1})G(g^p G(g^{p^2}, u), w)-1}{\pi^k}\right].$$

Let

$$\mu_{2,3} = \frac{1}{\zeta_1 - 1}\sum_{m=1}^{p-1}\frac{(1-u)^m}{m}.$$

$$\mu_{1,3} = \frac{1}{\zeta_1 - 1}\sum_{m=1}^{p-1}\frac{(1-\zeta_3^{-1}s^{-1})^m}{m}.$$

$$\mu_{1,2} = \frac{1}{\zeta_1 - 1}\sum_{m=1}^{p-1}\frac{(1-w)^m}{m}.$$

Conjecture 6.2.

$$R\left[\frac{g^{p^2}-1}{\pi^i}, \frac{g^p G(g^{p^2},u)-1}{\pi^j}, \frac{gG(g^{p^2},\zeta_3^{-1}s^{-1})G(g^p G(g^{p^2},u),w)-1}{\pi^k}\right]$$

$$= R\left[\frac{g^{p^2}-1}{\pi^i}, \frac{g^p(g^{p^2})^{[-\mu_{2,3}]}-1}{\pi^j}, \frac{g(g^{p^2})^{[-\mu_{1,3}]}(g^p(g^{p^2})^{[-\mu_{2,3}]})^{[-\mu_{1,2}]}-1}{\pi^k}\right].$$

Conjecture 6.3. *If* $\nu(\zeta_2 s^p - G(u^p, w)) \geq pi' + k$, *then* $\nu(\wp(\mu_{1,3}) + \mu_{1,2}\wp(\mu_{2,3})) \geq k - pi$.

We have

$$\begin{aligned} \nu(G(u^p, w) - 1) &= \nu(1 - u^p) + \nu(1 - w) - e' \\ &= \nu(\wp(\mu_{2,3})) + pe' + \nu(\mu_{1,2}) + e' - e' \\ &= \nu(\mu_{1,2}\wp(\mu_{2,3})) + pe', \end{aligned}$$

and

$$\nu(\zeta_2 s^p - 1) = \nu(\wp(\mu_{1,3})) + pe'.$$

Thus $\nu(\wp(\mu_{1,3}) + \mu_{1,2}\wp(\mu_{2,3})) + pe' \geq pi' + k$, which yields $\nu(\wp(\mu_{1,3}) + \mu_{1,2}\wp(\mu_{2,3})) \geq k - pi$.

Note:

$$\nu(\wp(\mu_{1,3}) + \mu_{1,2}\wp(\mu_{2,3})) \geq k - pi$$

is a familiar condition that has occurred in the classification of Hopf orders in $(KC_p^3)^*$ (see [BE18], [Ko17]).

References

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

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

[BE18], N. Byott, G. G. Elder, Sufficient conditions for large Galois scaffolds, *J. Num. Theory*, **182**, 2018, 95-130.

[Ch00], L. N. Childs, Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory, American Mathematical Society, Mathematical Surveys and Monographs **80**, 2000.

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

[El11], G. G. Elder, On the conjecture from truncated exponentials and Greither orders, *preprint dated August 2, 2011.*

[El12], G. G. Elder, Reversing the sense of Underwood's conjecture, *preprint dated February 24, 2012.*

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

[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.

[Ko17], A. Koch, Primitively generated Hopf orders in characteristic p, *Comm. Alg.*, **45**(6), 2017, 2673-2689.

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

[Mo93], S. Montgomery, Hopf Algebras and Their Actions on Rings, American Mathematical Society, CBMS Regional Conference Series in Mathematics, 82, (1993).

[T070], J. Tate, F. Oort, Group schemes of prime order, *Ann. Sci. Ec. Norm. Sup.*, **3**, (1970), 1-21.

[Un96], R. Underwood, The valuative condition and R-Hopf algebra orders in KC_{p^3}, *Amer. J. Math.*, **118**, (1996), 701-743.

[UC06], R. Underwood, L. N. Childs, Duality for Hopf orders, *Trans. Amer. Math. Soc.*, **358**(3), (2006), 1117-1163.

[Un06], R. Underwood, Realizable Hopf orders in KC_8, *Inter. Math. Forum*, **1**(17-20), (2006), 833-851.

[Un08], R. Underwood, Realizable Hopf orders in KC_{p^3}, *J. Algebra*, **319**, 2008, 4426-4455.

[Un11], R. Underwood, Truncated exponentials and Greither orders, *preprint dated June 24, 2011.*