Chapter 9
Hopf Orders in KC_{p^3}

In this chapter, we move on to the construction of Hopf orders in KC_{p^3}. We assume throughout this chapter that K is a finite extension of $\mathbb{Q}_p$ with $\zeta_{p^3} \in K$. Though all Hopf orders in KC_p and KC_{p^2} are known, this is not the case for Hopf orders in KC_{p^3}. L. Childs and R. Underwood have explored various ways to construct Hopf orders in KC_{p^3}; the reader is referred to the papers [CU03], [Un08b], [Un06], [UC05], and [Un96]. In the first section here, we briefly review the construction of "duality Hopf orders" of [UC05].

9.1 Duality Hopf Orders in KC_{p^3}

Let g be a generator for C_{p^3}, and let γ be a generator for $\hat{C}_{p^3}$. Let $\overline{g}$ denote the image of g under the mapping $KC_{p^3} \to KC_{p^2}$, $g^{p^2} \mapsto 1$, and let $\overline{\gamma}$ denote the image of γ under the mapping $K\hat{C}_{p^3} \to K\hat{C}_{p^2}$, $\gamma^{p^2} \mapsto 1$. For an integer m, $0 \leq m \leq e'$, set $m' = e' - m$, and, for a unit $u \in R$, set $\tilde{u} = \zeta_{p^2}^{-1} u^{-1}$. Let

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

and

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

be Greither orders in KC_{p^2}. Here u, w are units in R with

$$a_u = \sum_{l=0}^{p-1} u^l \frac{1}{p} \sum_{q=0}^{p-1} \zeta_p^{-lq} g^{p^2 q} \quad \text{and} \quad a_w = \sum_{l=0}^{p-1} w^l \frac{1}{p} \sum_{q=0}^{p-1} \zeta_p^{-lq} \overline{g}^{pq}.$$

Moreover, $pj \leq i$ and $pk \leq j$.

R.G. Underwood, *An Introduction to Hopf Algebras*, DOI 10.1007/978-0-387-72766-0_9,

By Proposition 8.3.9, the linear duals of these Hopf orders are Hopf orders in KC_{p^2} of the form

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

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

We shall extend the rank p^2 Hopf order $A(i,j,u)$ to obtain a Hopf order of rank p^3. To do this, we need to select a "correct" generator $\Psi \in KC_{p^3}$ that maps to $\dfrac{\overline{g}a_w - 1}{\pi^k}$ under the canonical surjection $KC_{p^3} \to KC_{p^2}$.

Let v be a unit of R, and let $a_v = \sum_{l=0}^{p-1} v^l \frac{1}{p} \sum_{q=0}^{p-1} \zeta_p^{-lq} g^{p^2 q}$. Let $\{e_{pm+n}\}$, $m,n = 0,\ldots,p-1$, denote the set of minimal idempotents in $K\langle g^p\rangle \cong KC_{p^2}$, and let

$$b_w = \sum_{m,n=0}^{p-1} w^m e_{pm+n}.$$

Note that

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

Let

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

Also, let x be a unit of R and let $a_x = \sum_{l=0}^{p-1} x^l \frac{1}{p} \sum_{q=0}^{p-1} \zeta_p^{-lq} \gamma^{p^2 q}$. Let $\{\iota_{pm+n}\}$, $m,n = 0,\ldots,p-1$, denote the set of minimal idempotents in $K\langle\gamma^p\rangle \cong K\hat{C}_{p^2}$, and let

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

and

$$J = A(k',j',i',\tilde{w},x,\tilde{u}) = A(k',j',\tilde{w})\left[\frac{\gamma a_x b_{\tilde{u}} - 1}{\pi^{i'}}\right].$$

We wish to find conditions on v and x such that H and J are R-orders in KC_{p^3} and $\langle H, J\rangle \subseteq R$. Then one can show that $\operatorname{disc}(J) = \operatorname{disc}(H^*)$. Thus, by Proposition 4.4.10, $J = H^*$ and H, J are Hopf orders.

First, we find conditions for H to be an R-order.

Lemma 9.1.1. *The algebra*

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

is an R-order in KC_{p^3} if the following inequalities hold:

(i) $\operatorname{ord}(v^p\zeta_{p^2} - 1) \geq i' + pk$;
(ii) $\operatorname{ord}(\tilde{u} - 1) \geq i' > 0$;
(iii) $\operatorname{ord}(\tilde{u} - 1) + \operatorname{ord}(w^p\zeta_p - 1) \geq e' + i' + pk$.

Proof. The conditions (i), (ii), and (iii) imply that $\dfrac{ga_vb_w - 1}{\pi^k}$ satisfies a monic polynomial of degree p with coefficients in $A(i, j, u)$ (see [UC05, §3]). Thus H is finitely generated over R. Thus, by [Rot02, Theorem 9.3], H is free and of finite rank over R. Clearly, $KH = KC_{p^3}$, and so H is an R-order. □

Similarly, we have the following lemma.

Lemma 9.1.2. *The algebra*

$$J = A(k', j', i', \tilde{w}, x, \tilde{u}) = R\left[\frac{\gamma^{p^2} - 1}{\pi^{k'}}, \frac{\gamma^p a_{\tilde{w}} - 1}{\pi^{j'}}, \frac{\gamma a_x b_{\tilde{u}} - 1}{\pi^{i'}}\right]$$

is an R-order in $K\hat{C}_{p^3}$ if the following inequalities hold:

(i) $\operatorname{ord}(x^p\zeta_{p^2} - 1) \geq k + pi'$;
(ii) $\operatorname{ord}(w - 1) \geq k > 0$;
(iii) $\operatorname{ord}(w - 1) + \operatorname{ord}(\tilde{u}^p\zeta_p - 1) \geq e' + k + pi'$.

Proof. The conditions (i), (ii), and (iii) imply that $\dfrac{\gamma a_x b_{\tilde{w}} - 1}{\pi^k}$ satisfies a monic polynomial with coefficients in $A(k', j', \tilde{w})$ (see [UC05, §3]). Thus J is free and of finite rank over R. Since $KJ = K\hat{C}_{p^3}$, J is an R-order in $K\hat{C}_{p^3}$. □

With some additional conditions, we can show that J and H are dual Hopf orders in KC_{p^3}. For $a, b \in R$, let $G(a, b)$ denote the **Gauss sum of a and b**, defined as

$$G(a, b) = \frac{1}{p}\sum_{m=0}^{p-1}\sum_{n=0}^{p-1}\zeta_p^{-mn}a^n b^m.$$

Proposition 9.1.1. *Let $H = A(i, j, k, u, v, w)$ and $J = A(k', j', i', \tilde{w}, x, \tilde{u})$ be R-algebras that satisfy the hypotheses of Lemmas 9.1.1 and 9.1.2, with the additional conditions*

(i) $e' > \operatorname{ord}(w - 1)$,
(ii) $e' > \operatorname{ord}(\tilde{u} - 1)$,
(iii) $\operatorname{ord}(w - 1) + \operatorname{ord}(\tilde{u} - 1) \geq e' + (\frac{p-1}{p})(i' + k + e')$, *and*
(iv) $vx\zeta_{p^3}G(\tilde{u}, w) = 1$.

Then H and J are Hopf orders in KC_{p^3} with $J = H^*$.

Proof. By Lemma 9.1.1, H is an R-order in KC_{p^3}, and, by Lemma 9.1.2, J is an R-order in $K\hat{C}_{p^3}$. The conditions (i)–(iv) above imply that $\langle J, H\rangle \subseteq R$. Moreover, $\operatorname{disc}(H^*) = \operatorname{disc}(J)$. (For details of these calculations, see [UC05, §3].) Thus H and $J = H^*$ are Hopf orders by Proposition 4.4.10. □

The Hopf orders constructed in Proposition 9.1.1 are called **duality Hopf orders** in KC_{p^3}.

For p prime, the group ring KC_{p^3} is a K-Hopf algebra. There exists a Hopf inclusion $KC_{p^2} \cong K\langle g^p\rangle \to KC_{p^3}$, and a Hopf surjection $KC_{p^3} \overset{g^p\mapsto 1}{\to} K\langle \overline{g}\rangle \cong KC_p$, with

$$KC_{p^3}/i(K\langle g^p\rangle^+)KC_{p^3} \cong K\langle \overline{g}\rangle,$$

and thus there is a short exact sequence

$$K \to K\langle g^p\rangle \to KC_{p^3} \overset{g^p\mapsto 1}{\to} K\langle \overline{g}\rangle \to K. \tag{9.1}$$

At the same time, there exists a Hopf inclusion $KC_p \cong K\langle g^{p^2}\rangle \to KC_{p^3}$, and a Hopf surjection $KC_{p^3} \overset{g^{p^2}\mapsto 1}{\to} K\langle \overline{g}\rangle \cong KC_{p^2}$, with

$$KC_{p^3}/i(K\langle g^{p^2}\rangle^+)KC_{p^3} \cong K\langle \overline{g}\rangle,$$

and thus there is a short exact sequence

$$K \to K\langle g^{p^2}\rangle \to KC_{p^3} \overset{g^{p^2}\mapsto 1}{\to} K\langle \overline{g}\rangle \to K. \tag{9.2}$$

Proposition 9.1.2. *Let $A(i,j,k,u,v,w)$ be a duality Hopf order in KC_{p^3}. Then there exist short exact sequences of R-Hopf orders*

$$R \to A(i,j,u) \to A(i,j,k,u,v,w) \to H(k) \to R, \tag{9.3}$$

$$R \to H(i) \to A(i,j,k,u,v,w) \to A(j,k,w) \to R. \tag{9.4}$$

Proof. One shows that $A(i,j,k,u,v,w) \cap K\langle g^p\rangle = A(i,j,u)$ and that the image of $A(i,j,k,u,v,w)$ is $H(k)$ under the map given by $g^p \mapsto 1$. Thus (9.3) is a short exact sequence by §4.4 (4.10).

Moreover, $A(i,j,k,u,v,w) \cap K\langle g^{p^2}\rangle = H(i)$, and the image of $A(i,j,k,u,v,w)$ under the map given by $g^{p^2} \mapsto 1$ is $A(j,k,w)$, and so (9.4) is a short exact sequence by §4.4 (4.10). We leave the details to the reader as an exercise. □

If H is an arbitrary R-Hopf order in KC_{p^3}, then the extensions (9.1) and (9.2) induce extensions of R-Hopf orders,

$$R \to A(i,j,u) \to H \to H(k) \to R \tag{9.5}$$

and

$$R \to H(i) \to H \to A(j,k,w) \to R, \tag{9.6}$$

for R-Hopf orders $A(i, j, u)$ and $A(j, k, w)$. The sequence (9.6) dualizes to yield the short exact sequence

$$R \to A(k', j', \tilde{w}) \to H^* \to H(i') \to R. \tag{9.7}$$

In an effort to classify all Hopf orders in KC_{p^3}, R. Underwood has given the following analog of Definition 8.1.1 for Hopf orders in KC_{p^3}.

Definition 9.1.1. Let H be an R-Hopf order in KC_{p^3} inducing the short exact sequences (9.5) and (9.7) as above. Let $\Xi(A(i, j, u))$ denote the p-adic obgv determined by $A(i, j, u)$, and let $\Xi(A(k', j'\tilde{w}))$ denote the p-adic obgv given by $A(k', j', \tilde{w})$ (see Proposition 5.3.9). Then H satisfies the **valuation condition for** $n = 3$ if either

$$pk \leq \Xi(A(i, j, u))(g^p)$$

or

$$pi' \leq \Xi(A(k', j', \tilde{w}))(\gamma^p).$$

To see Definition 9.1.1 as an extension of Definition 8.1.1, let

$$R \to H(i) \to H \to H(j) \to R$$

and

$$R \to H(j') \to H^* \to H(i') \to R$$

be short exact sequences, where H is an R-Hopf order in KC_{p^2}. Then H satisfies the valuation condition for $n = 2$ if and only if either

$$pj \leq \Xi(H(i))(\tau),\ \langle\tau\rangle = C_p,$$

or

$$pi' \leq \Xi(H(j'))(\eta),\ \langle\eta\rangle = \hat{C}_p,$$

since $\Xi(H(i))(\tau) = i$ and $\Xi(H(j'))(\eta) = j'$.

In [UC05], the authors show that every duality Hopf order $A(i, j, k, u, v, w)$ satisfies the valuation condition for $n = 3$ (see [UC05, Theorem 3.8]), and it has been conjectured that an arbitrary Hopf order in KC_{p^3} satisfies the valuation condition. Indeed, there are no known examples where the condition fails.

9.2 Circulant Matrices and Hopf Orders in KC_{p^3}

In this section, we construct another collection of Hopf orders in KC_{p^3}. We keep the notation of the previous section: $\overline{g}$ denotes the image of g under the mapping $KC_{p^3} \to KC_{p^2}$, $g^{p^2} \mapsto 1$, and $\overline{\gamma}$ denotes the image of γ under the mapping

$K\hat{C}_{p^3} \to K\hat{C}_{p^2}$, $\gamma^{p^2} \mapsto 1$. For an integer $n \geq 1$, let $\langle\ ,\rangle_n$ denote the duality map $K\hat{C}_{p^n} \times KC_{p^n} \to K$. For an integer m, $0 \leq m \leq e'$, let $m' = e' - m$, and for a unit $u \in R$, let $\tilde{u} = \zeta_{p^2}^{-1} u^{-1}$.

Let

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

and

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

be Hopf orders in KC_{p^2} with linear duals

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

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

We assume that $j' > pi'$, $j + i' > \mathrm{ord}(1-\tilde{u})$ and $j' + k > \mathrm{ord}(1-w)$.

We construct our collection of Hopf orders by choosing generators $\Psi \in KC_{p^3}$ and $\Phi \in K\hat{C}_{p^3}$ such that the R-modules $H = A(i,j,u)[\Psi]$ and $J = A(k',j',\tilde{w})[\Phi]$ are invariant under the comultiplications of KC_{p^3} and $K\hat{C}_{p^3}$, respectively. We also require that $\langle J, H\rangle_3 \subseteq R$. Then, as we shall see, H and $J = H^*$ are Hopf orders in KC_{p^3}.

We begin with the construction of Ψ. Let

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

$$\rho_q = \frac{1}{p}\sum_{n=0}^{p-1} \zeta_p^{-qn}\overline{\gamma}^{pn}, \quad 0 \leq q \leq p-1,$$

and

$$e_{pm+n} = \frac{1}{p^2}\sum_{a=0}^{p-1}\sum_{b=0}^{p-1} \zeta_{p^2}^{-(pm+n)(pa+b)} g^{p(pa+b)}$$

denote the idempotents for $K\langle\gamma^p\rangle \cong K\hat{C}_{p^2}$, $K\langle\overline{\gamma}^p\rangle \cong K\hat{C}_p$, and $K\langle g^p\rangle \cong KC_{p^2}$, 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 indeterminate, and set

$$x = \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} x_{pm+n} e_{pm+n}, \quad x_{pm} = w^m.$$

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

$$\left\langle (\gamma^{p^2} - 1)^q (\gamma^p a_{\tilde{w}} - 1)^r (\gamma\tau - 1)^s, gx - 1 \right\rangle_3 = 0 \tag{9.8}$$

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

Lemma 9.2.1. *The solution to* (9.8) is a vector (x_{pm+n}), $0 \le m, n \le p-1$, of elements of R defined as

$$x_{pm+n} = \zeta_{p^3}^{-n} s_1^{-n} \langle \overline{\gamma}^{pm} d^{-n}, a_w \rangle_1.$$

Proof. One has

$$(\gamma^{p^2}-1)^q (\gamma^p a_{\tilde{w}}-1)^r (\gamma\tau-1)^s = \sum_{m,n=0}^{p-1} \left(\zeta_p^n - 1\right)^q \left(\zeta_{p^2}^{pm+n} \tilde{w}^n - 1\right)^r (\gamma s_{pm+n} - 1)^s \iota_{pm+n}$$

and

$$\langle \gamma^t \iota_{pm+n}, g e_{pa+b} \rangle = \begin{cases} \dfrac{1}{p} \zeta_{p^3}^t \zeta_p^{-ma} & \text{if } n = 1, b = t \\ 0 & \text{otherwise,} \end{cases}$$

and thus (9.8) expands to

$$(\zeta_p - 1)^q \sum_{m=0}^{p-1} \left(\zeta_{p^2}^{pm+1} \tilde{w} - 1\right)^r \sum_{t=0}^{s} \binom{s}{t} (-1)^{s-t} s_{pm+1}^t \sum_{a=0}^{p-1} x_{pa+t} \left(\frac{1}{p} \zeta_{p^3}^t \zeta_p^{-ma}\right) = 0. \tag{9.9}$$

For integers $l, n = 0, \ldots, p-1$, let

$$h_l^{(n)} = \frac{1}{p} \sum_{q=0}^{p-1} \zeta_p^{-lq} s_{pq+1}^n.$$

Then (9.9) can be rewritten as

$$\sum_{y=0}^{r}\binom{r}{y}(-1)^{r-y}\zeta_{p^2}^{y}\tilde{w}^{y}\sum_{n=0}^{s}\binom{s}{n}(-1)^{s-n}\zeta_{p^3}^{n}\sum_{l=0}^{p-1}x_{pl+n}h_{l-y}^{(n)}=0, \tag{9.10}$$

where the subscripts on $h_{l-y}^{(n)}$ are read modulo p.
Equation (9.10) is equivalent to the system

$$\begin{cases}\zeta_{p^3}^{n}\left(h_0^{(n)}x_n+h_1^{(n)}x_{p+n}+\cdots+h_{p-1}^{(n)}x_{(p-1)p+n}\right) & =1\\ \zeta_{p^3}^{n}\tilde{w}\zeta_{p^2}\left(h_{p-1}^{(n)}x_n+h_0^{(n)}x_{p+n}+\cdots+h_{p-2}^{(n)}x_{(p-1)p+n}\right) & =1\\ \zeta_{p^3}^{n}\left(\tilde{w}\zeta_{p^2}\right)^2\left(h_{p-2}^{(n)}x_n+h_{p-1}^{(n)}x_{p+n}+\cdots+h_{p-3}^{(n)}x_{(p-1)p+n}\right) & =1\\ \qquad\vdots & \\ \zeta_{p^3}^{n}\left(\tilde{w}\zeta_{p^2}\right)^{p-1}\left(h_1^{(n)}x_n+h_2^{(n)}x_{p+n}+\cdots+h_0^{(n)}x_{(p-1)p+n}\right) & =1.\end{cases} \tag{9.11}$$

In matrix form, (9.11) appears as

$$\begin{pmatrix}h_0^{(n)} & h_1^{(n)} & h_2^{(n)} & \dots & h_{p-1}^{(n)}\\ h_{p-1}^{(n)} & h_0^{(n)} & h_1^{(n)} & \dots & h_{p-2}^{(n)}\\ h_{p-2}^{(n)} & h_{p-1}^{(n)} & h_0^{(n)} & \dots & h_{p-3}^{(n)}\\ \vdots & \vdots & & & \vdots\\ h_1^{(n)} & h_2^{(n)} & h_3^{(n)} & \dots & h_0^{(n)}\end{pmatrix}\begin{pmatrix}x_n\\ x_{p+n}\\ x_{2p+n}\\ \vdots\\ x_{(p-1)p+n}\end{pmatrix}=\begin{pmatrix}\zeta_{p^3}^{-n}\\ w\zeta_{p^3}^{-n}\\ w^2\zeta_{p^3}^{-n}\\ \vdots\\ w^{p-1}\zeta_{p^3}^{-n}\end{pmatrix}. \tag{9.12}$$

Here the coefficient matrix is the circulant matrix

$$M^{(n)}=\operatorname{circ}\left(h_0^{(n)},h_1^{(n)},h_2^{(n)},\dots,h_{p-1}^{(n)}\right).$$

Note that the eigenvalues of $M^{(n)}$ are $s_{pq+1}^{n}\neq 0$, for $0\leq q\leq p-1$, with corresponding eigenvectors (ζ_p^{lq}), $0\leq l\leq p-1$. Thus $M^{(n)}$ is invertible with inverse $\Theta^{(n)}=(\theta_{m,l}^{(n)})$ for $m,l=0,\dots,p-1$. Consequently, the matrix equations in (9.12) have unique solutions for $m,n=0,\dots,p-1$, $n>0$. These solutions are computed to be

$$x_{pm+n}=\zeta_{p^3}^{-n}s_1^{-n}\langle\overline{\gamma}^{pm}d^{-n},a_w\rangle_1.$$

□

Now let $u_{pm+n} = x_{pm+n}$, $n > 0$, and let

$$b = \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} u_{pm+n} e_{pm+n}, \quad u_{pm} = w^m.$$

Put

$$\Psi = \frac{gb-1}{\pi^k},$$

and let

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

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

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

Lemma 9.2.2. *Let H be the R-module as above. Suppose*

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

(ii) $\operatorname{ord}\left(\zeta_{p^2} s_1^p \langle \overline{\gamma}^p d^p, a_w \rangle_1 - 1\right) \geq pi' + k$, *and*

(iii) $\operatorname{ord}(\zeta_{p^3} s_1 - 1) \geq i' + \dfrac{k}{p^2}$.

Then H is invariant under the comultiplication of KC_{p^3}.

Proof. (Sketch.) We show that $\Delta_{KC_{p^3}}(H) \subseteq H \otimes_R H$. Since

$$\Delta_{KC_{p^3}}(\Psi) = \Psi \otimes 1 + 1 \otimes \Psi + \pi^k \Psi \otimes \Psi + \frac{\Delta(gb) - gb \otimes gb}{\pi^k},$$

H is invariant under $\Delta = \Delta_{KC_{p^3}}$ if and only if

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

The condition $j' > pi'$ guarantees that $A(i,j,u) \neq RC_{p^2}^*$, and so, by Chapter 4, Exercise 12, $A(i,j,u)$ is a local ring with maximal ideal $(\pi, A(i,j,u)^+)$. One has $b \in A(i,j,u)$ and $b \notin (\pi, A(i,j,u)^+)$, and so b is a unit in $A(i,j,u)$. Thus g is a unit in H. Therefore H is invariant under $\Delta_{KC_{p^3}}$ if and only if

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

which follows from the conditions of the lemma. The reader is referred to [Un08b, Lemma 2.6] for the details of this computation. □

Our next task is to construct Φ. Suppose that $H = A(i, j, u)[\dfrac{gb-1}{\pi^k}]$ is an R-module as constructed by Lemma 9.2.2, with $b = \sum_{m=0}^{p-1}\sum_{n=0}^{p-1} u_{pm+n}e_{pm+n}$. Set $c = \sum_{m=0}^{p-1} u_1^{-1}u_{pm+1}f_m$, where f_m are the minimal idempotents in $K\langle\overline{g}^p\rangle \cong KC_p$. The quantities c and f_m are the analogs in the dual situation for d and ρ_q. Let y_{pm+n}, $m, n = 0, \ldots, p-1$ be indeterminate, 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 above, we find values for y_{pm+n}, $n > 0$, for which

$$\left\langle \gamma y - 1, \left(g^{p^2} - 1\right)^l (g^p a_u - 1)^m (gb-1)^t \right\rangle = 0 \tag{9.13}$$

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

Lemma 9.2.3. *The solution to* (9.13) *is a vector* (y_{pm+n}), $0 \le m, n \le p-1$, *of elements of* R *defined as*

$$y_{pm+n} = \zeta_{p^3}^{-n} u_1^{-n}\langle \overline{g}^{pm} c^{-n}, a_{\tilde{u}}\rangle$$

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

Proof. We follow the method of Lemma 9.2.1. For integers $l, n = 0, \ldots, p-1$, define $\eta_l^{(n)}$ as

$$\eta_l^{(n)} = \frac{1}{p}\sum_{q=0}^{p-1} \zeta_p^{-lq} u_{pq+1}^n.$$

Then, finding quantities y_{pm+n} that satisfy (9.13) is equivalent to solving the matrix equations for $n = 1, 2, 3, \ldots, p-1$:

$$\begin{pmatrix} \eta_0^{(n)} & \eta_1^{(n)} & \eta_2^{(n)} & \ldots & \eta_{p-1}^{(n)} \\ \eta_{p-1}^{(n)} & \eta_0^{(n)} & \eta_1^{(n)} & \ldots & \eta_{p-2}^{(n)} \\ \eta_{p-2}^{(n)} & \eta_{p-1}^{(n)} & \eta_0^{(n)} & \ldots & \eta_{p-3}^{(n)} \\ \vdots & \vdots & & & \vdots \\ \eta_1^{(n)} & \eta_2^{(n)} & \eta_3^{(n)} & \ldots & \eta_0^{(n)} \end{pmatrix} \begin{pmatrix} y_n \\ y_{p+n} \\ y_{2p+n} \\ \vdots \\ y_{(p-1)p+n} \end{pmatrix} = \begin{pmatrix} \zeta_{p^3}^{-n} \\ \tilde{u}\zeta_{p^3}^{-n} \\ \tilde{u}^2\zeta_{p^3}^{-n} \\ \vdots \\ \tilde{u}^{p-1}\zeta_{p^3}^{-n} \end{pmatrix}. \tag{9.14}$$

Here the coefficient matrix is the circulant matrix

$$N^{(n)} = \operatorname{circ}\left(\eta_0^{(n)}, \eta_1^{(n)}, \eta_2^{(n)}, \ldots, \eta_{p-1}^{(n)}\right).$$

Let $\Phi^{(n)} = (\phi_{m,l}^{(n)})$, $m, l = 0, \ldots, p-1$ denote the inverse of $N^{(n)}$. Then the matrix equations in (9.14) have unique solutions,

$$\begin{aligned} y_{pm+n} = v_{pm+n} &= \zeta_{p^3}^{-n} \sum_{l=0}^{p-1} \phi_{m,l}^{(n)} \tilde{u}^l \\ &= \zeta_{p^3}^{-n} u_1^{-n} \langle \overline{g}^{pm} c^{-n}, a_{\tilde{u}} \rangle, \end{aligned}$$

for $m, n = 0, \ldots, p-1, n > 0$. □

Now, let

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

put

$$\Phi = \frac{\gamma\beta - 1}{\pi^{i'}},$$

and let

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

denote the R-module that is the $A(k', j', \tilde{w})$-span of the set

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

Lemma 9.2.4. *Suppose H satisfies the hypothesis of Lemma 9.2.2. 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 invariant under the comultiplication of $K\hat{C}_{p^3}$.*

Proof. We use the criteria of Lemma 9.2.2 to show that $\Delta_{K\hat{C}_{p^3}}(J) \subseteq J \otimes_R J$. In this case, J is invariant if $j > pk$,

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

$$\operatorname{ord}\left(\zeta_{p^2} u_1^p \langle \overline{g}^p c^p, a_{\tilde{u}} \rangle - 1\right) \geq pk + i',$$

and

$$\operatorname{ord}(\zeta_{p^3}u_1 - 1) \geq k + \frac{i'}{p^2},$$

which follow from the conditions of the lemma. Details of the computations are found in [Un08b, Lemma 2.7].

Let $H = A(i, j, u)\left[\frac{gb-1}{\pi^k}\right]$ and $J = A(k', j', \tilde{w})[\frac{\gamma\beta - 1}{\pi^{i'}}]$ be R-modules as constructed above by Lemma 9.2.2 and Lemma 9.2.4. We need several more lemmas before we can show that H and J are Hopf orders.

Let

$$H^* = \{\alpha \in K\hat{C}_{p^3} : \langle \alpha, H\rangle_3 \subseteq R\}$$

denote the linear dual of the R-module H.

Lemma 9.2.5. *H^* is an R-algebra.*

Proof. By Lemma 9.2.2, $\Delta_{KC_{p^3}} : H \to H \otimes H$. Thus there is a map of linear duals $\Delta^*_{KC_{p^3}} : (H \otimes_R H)^* \to H^*$. Since $H^* \otimes_R H^* \subseteq (H \otimes_R H)^*$, $\Delta^*_{KC_{p^3}}$ serves as multiplication on H^*. □

Lemma 9.2.6. *Let $\overline{H}$ be the image of H under the mapping $KC_{p^3} \to KC_{p^2}$, $g^{p^2} \mapsto 1$. Then*

$$K\hat{C}_{p^2} \cap H^* = \overline{H}^* = A(j, k, w)^* = A(k', j', \tilde{w}).$$

Proof. We show that $\overline{H}^* = K\hat{C}_{p^2} \cap H^*$. Let $\alpha \in \overline{H}^*$. Then $\alpha \in K\hat{C}_{p^2}$ and $\langle \alpha, \overline{H}\rangle_2 \subseteq R$. Let $f \in H$, and let $\overline{f}$ be the image of f under the mapping $KC_{p^3} \to KC_{p^2}$. Then $\langle \alpha, f\rangle_3 = \langle \alpha, \overline{f}\rangle_2$. Hence

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

so that $\alpha \in H^*$. Hence $\alpha \in K\hat{C}_{p^2} \cap H^*$.

Now suppose $\alpha \in K\hat{C}_{p^2} \cap H^*$. Then $\alpha \in K\hat{C}_{p^2}$ and $\langle \alpha, H\rangle_3 \subseteq R$. Consequently, $\alpha \in \overline{H}^*$, which shows that $\overline{H}^* = K\hat{C}_{p^2} \cap H^*$.

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

Lemma 9.2.7. $J \subseteq H^*$.

Proof. By Lemma 9.2.5, H^* is an algebra. Thus it suffices to show that $A(k', j', \tilde{w}) \subseteq H^*$ and $\dfrac{\gamma\beta - 1}{\pi^{i'}} \in H^*$. By Lemma 9.2.6, $H^* \cap K\hat{C}_{p^2} = A(k', j', \tilde{w})$, and thus $A(k', j', \tilde{w}) \subseteq H^*$. We claim that $\dfrac{\gamma\beta - 1}{\pi^{i'}} \in H^*$, but this amounts to showing that

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

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

$$\operatorname{ord}\left(\left\langle \gamma\beta-1,\left(g^{p^2}-1\right)^{l}\left(g^{p}a_u-1\right)^{m}(gb-1)^{t}\right\rangle\right)\geq i'+li+mj+tk \quad (9.15)$$

for $l,m,t=0,\ldots,p-1$, $t>0$. But (9.15) is satisfied since (9.13) holds with $y=\beta$. □

Proposition 9.2.1. *Let $A(i,j,u)$ and $A(j,k,w)$ be Hopf orders in KC_{p^2} with linear duals $A(j',i',\tilde{u})$ and $A(k',j',\tilde{w})$, respectively. Let s be a unit of R, and put $s_{pm+n}=s^n\tilde{u}^m$ for $m,n=0,\ldots,p-1$. Let*

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

Let

$$b=\sum_{m=0}^{p-1}\sum_{n=0}^{p-1}u_{pm+n}e_{pm+n},$$

where $u_{pm+n}=\zeta_{p^3}^{-n}s^{-n}G(\zeta_p^m\tilde{u}^{-n},w)$.

Suppose

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

satisfies

$$\left\langle \gamma\beta-1,\left(g^{p^2}-1\right)^{l}\left(g^{p}a_u-1\right)^{m}(gb-1)^{t}\right\rangle=0$$

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

Additionally, suppose the following conditions are satisfied:

(i) $\operatorname{ord}\left(\zeta_{p^2}s^pG(u^{-p},w)-1\right)\geq pi'+k$;

(ii) $\operatorname{ord}(\zeta_{p^3}s-1)\geq i'+\dfrac{k}{p^2}$;

(iii) $i\geq pj$;

(iv) $j'>pi'$;

(v) $k'\geq p^2i'$;

(vi) $j\geq p^2k>pk$;

(vii) $e'\geq i+j+k$.

Then $H=A(i,j,u)\left[\frac{gb-1}{\pi^k}\right]$ is a Hopf order in KC_{p^3} with linear dual $J=A(k',j',\tilde{w})\left[\frac{\gamma\beta-1}{\pi^{i'}}\right]$.

Proof. Conditions (i)–(vii) show that $\Delta_{KC_{p^3}}(H) \subseteq H \otimes_R H$ and $\Delta_{K\hat{C}_{p^3}}(J) \subseteq J \otimes_R J$.

We show that J is an R-Hopf order. By Lemmas 9.2.5 and 9.2.6, H^* is an R-algebra with $H^* \cap K\hat{C}_{p^2} = A(k', j', \tilde{w})$. By Lemma 9.2.7, $\frac{\gamma\beta-1}{\pi^{i'}} \in H^*$. Thus $\frac{\gamma\beta-1}{\pi^{i'}}$ satisfies a monic polynomial of degree p with coefficients in $A(k', j', \tilde{w})$. Thus J is an R-algebra, and consequently J is an R-Hopf order.

By Lemma 9.2.7, $H \subseteq J^*$. Since $J^* \cap KC_{p^2} = A(i, j, u)$, $\frac{gb-1}{\pi^k}$ satisfies a monic polynomial of degree p with coefficients in $A(i, j, u)$. Thus H is an R-Hopf order. An application of Proposition 7.1.3 then shows that $H^* = J$.

In light of the fact that circulant matrices play a key role in their construction, we call the Hopf orders constructed in Proposition 9.2.1 **circulant matrix Hopf orders** in KC_{p^3}.

9.3 Chapter Exercises

Exercises for §9.1

1. Let K be a finite extension of $\mathbb{Q}_p$. Show that there are Larson orders in KC_{p^3} that are not duality Hopf orders.
2. Let K be a finite extension of $\mathbb{Q}_2$. Construct an example of a duality Hopf order in KC_8.
3. In the construction of the duality Hopf orders, prove that either $A(j, k, w)$ or $A(j', i', \tilde{u})$ is a Larson order.
4. Compute the p-adic obgv determined by an arbitrary duality Hopf order.
5. Give the details in the proof of Proposition 9.1.2.

Exercises for §9.2

6. Prove that every Larson order in KC_{p^3} is a circulant matrix Hopf order.
7. Construct an example of a circulant matrix Hopf order in KC_8.
8. Prove that there exist circulant matrix Hopf orders that are not duality.
9. Prove that there exist duality Hopf orders that are not circulant matrix.
10. Does the valuation condition for $n = 3$ hold for the collection of circulant matrix Hopf orders?