Chapter 8
Hopf Orders in KC_{p^2}

In this chapter, we assume that K is a finite extension of $\mathbb{Q}_p$, containing ζ_{p^2}, endowed with the discrete valuation ord. Set $e = \text{ord}(p)$, $e' = e/(p-1)$. Let g be a generator for C_{p^2}.

8.1 The Valuation Condition

The K-Hopf algebra KC_{p^2} induces the short exact sequence of K-Hopf algebras

$$K \xrightarrow{\lambda} KC_p \xrightarrow{i} KC_{p^2} \xrightarrow{s} KC_p \xrightarrow{\epsilon} K,$$

where $i : KC_p \to KC_{p^2}$ is the Hopf inclusion and $s : KC_{p^2} \to KC_p$ is the Hopf surjection, given as $g^p \mapsto 1$. Let H denote an R-Hopf order in KC_{p^2}. Since $H' = H \cap KC_p$ is an R-Hopf order in KC_p and $H'' = s(H)$ is an R-Hopf order in KC_p, one has the short exact sequence of Hopf orders

$$R \to H' \to H \to H'' \to R. \tag{8.1}$$

By Proposition 7.1.2, H' and H'' are Larson orders in KC_p of the form

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

where i, j are integers satisfying $0 \le i, j \le e'$. Thus (8.1) can be written as

$$R \to H(i) \to H \to H(j) \to R. \tag{8.2}$$

By Proposition 4.3.3, H has a generating integral Λ, which we now compute.

R.G. Underwood, *An Introduction to Hopf Algebras*, DOI 10.1007/978-0-387-72766-0_8,

Proposition 8.1.1. *The ideal of integrals* $\int_H$ *is of the form* $R\Lambda$*, where*

$$\Lambda = \frac{p^2}{\pi^{(p-1)(i+j)}} e_0,$$

where $e_0 = \frac{1}{p^2} \sum_{m=0}^{p^2-1} g^m$.

Proof. By Proposition 4.4.5, $\int_H = \epsilon_H \left(\int_H\right) e_0$, and so, by Proposition 4.4.12,

$$\int_H = \epsilon_{H(i)} \left(\int_{H(i)}\right) \epsilon_{H(j)} \left(\int_{H(j)}\right) e_0.$$

Now, by Proposition 5.3.3, $\epsilon_{H(i)} \left(\int_{H(i)}\right) = \frac{p}{\pi^{(p-1)i}} R$, and $\epsilon_{H(j)} \left(\int_{H(j)}\right) = \frac{p}{\pi^{(p-1)j}} R$. Thus $\int_H = R\Lambda$ with

$$\Lambda = \frac{p^2}{\pi^{(p-1)(i+j)}} e_0.$$

□

By Proposition 7.1.4,

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

and the sequence (8.2) can be dualized (see (4.13)) to form the short exact sequence

$$R \to H(j') \xrightarrow{s^*} H^* \xrightarrow{i^*} H(i') \to R.$$

Definition 8.1.1. Let H be an R-Hopf order in KC_{p^2} that induces the short exact sequence (8.2). Then H satisfies the **valuation condition for** $n = 2$ if either $pj \leq i$ or $pi' \leq j'$.

In the paper [Lar88], R. Larson proved that every Hopf order in KC_4 satisfies the valuation condition. In [Un94], R. Underwood showed that the valuation condition holds for Hopf orders in KC_{p^2}, $p \geq 2$. Underwood's result also follows from results of N. Byott; see [By93b, §8, Theorem 5]. In this section, we prove that the valuation condition holds for Hopf orders in KC_{p^2}, following closely the proof in [Un94].

We first prove that the valuation condition holds for H that induces short exact sequences (8.2) with $i \geq e/p$. The key is to obtain an R-basis for H^* in a special form.

Lemma 8.1.1. *Let* H *be an* R*-Hopf order in* KC_{p^2} *inducing the short exact sequence* (8.2) *with* $i \geq e/p$. *Let* $h = \frac{\gamma^p - 1}{\pi^{e'}}$, $k = \frac{\gamma - 1}{\pi^{i'}}$. *Put*

$$X = \big(k, k^2, \ldots, k^{p-1}, hk, hk^2, \ldots, hk^{p-1}, \ldots, h^{p-1}k, h^{p-1}k^2, \ldots, h^{p-1}k^{p-1}, 1, h, \ldots, h^{p-1}\big).$$

Then there exists an R-basis $\{\alpha_m\}_{m=1}^{p^2}$ for H^* given by the matrix product

$$XM' = (\alpha_1, \alpha_2, \ldots, \alpha_{p^2}),$$

where M' is the $p^2 \times p^2$ matrix

$$M' = \begin{pmatrix} r_{1,1} & r_{1,2} & \cdots & \cdots & r_{1,p^2} \\ 0 & r_{2,2} & \cdots & \cdots & r_{2,p^2} \\ \vdots & \vdots & & & \vdots \\ 0 & 0 & \cdots & \cdots & r_{p^2,p^2} \end{pmatrix},$$

which satisfies the following conditions:

(i) *either $r_{l,m} = 0$ or $\mathrm{ord}(r_{l,m}) > \mathrm{ord}(r_{l,m+1})$ for all $1 \le l, m \le p^2 - 1$;*
(ii) *$\mathrm{ord}(r_{l,m}) \ge aj + bi' - (p-1)i'$ for $1 \le m \le p^2 - p$, where $l = a(p-1) + b$ for $0 \le a \le p-1$, $1 \le b \le p-1$.*

Proof. Since $H(i)$ injects into H, and $RC_{p^2} \subseteq H$, the Larson order $H(i,0)$ is contained in H. Thus

$$H^* \subseteq H(i,0)^* = R\left[\frac{\gamma^p - 1}{\pi^{e'}}, \frac{\gamma u - 1}{\pi^{i'}}\right],$$

where $u = \Sigma_{m=0}^{p-1} \zeta_{p^2}^{-m} \iota_m$ by Proposition 7.1.5. But, since $i \ge e/p$, Lemma 7.1.6 implies that

$$\frac{u-1}{\pi^{i'}} = \frac{1}{\pi^{i'}} \sum_{m=0}^{p-1} \left(\zeta_{p^2}^{-m} - 1\right) \iota_m \in H(e').$$

Thus

$$R\left[\frac{\gamma^p - 1}{\pi^{e'}}, \frac{\gamma u - 1}{\pi^{i'}}\right] = R\left[\frac{\gamma^p - 1}{\pi^{e'}}, \frac{\gamma - 1}{\pi^{i'}}\right],$$

and so $H^* \subseteq H(e', i') = R\left[\frac{\gamma^p - 1}{\pi^{e'}}, \frac{\gamma - 1}{\pi^{i'}}\right]$. One has that X is an R-basis for $H(e', i')$. Therefore, an R-basis $\{\alpha_m\}_{m=1}^{p^2}$ for H^* is given by the matrix product

$$XM = (\alpha_1, \alpha_2, \ldots, \alpha_{p^2}),$$

where M is a $p^2 \times p^2$ matrix with entries in R. Performing elementary column operations on M, one sees that it is column-equivalent to the matrix

$$M' = \begin{pmatrix} r_{1,1} & r_{1,2} & \cdots & \cdots & r_{1,p^2} \\ 0 & r_{2,2} & \cdots & \cdots & r_{2,p^2} \\ \vdots & \vdots & & & \vdots \\ 0 & 0 & \cdots & \cdots & r_{p^2,p^2} \end{pmatrix},$$

where either $r_{l,m} = 0$ or $\text{ord}(r_{l,m}) > \text{ord}(r_{l,m+1})$ for all $1 \le l, m \le p^2 - 1$. Thus $\{\alpha_m\}_{m=1}^{p^2}$ defined by

$$XM' = (\alpha_1, \alpha_2, \ldots, \alpha_{p^2})$$

is an R-basis for H^*. Note that M' satisfies condition (i) of the lemma.

We now show that M' satisfies condition (ii).

We have

$$\alpha_m = \sum_{l=a(p-1)+b}^{p^2-p} r_{l,m} h^a k^b + \sum_{\iota=p^2-p+1}^{p^2} r_{\iota,m} h^{\iota-p^2+p-1}$$

for $m = 1, \ldots, p^2$, $0 \le a \le p-1$, $1 \le b \le p-1$. Since M' is upper-triangular, $r_{l,m} = 0$ for $l = m+1, \ldots, p^2$. By Proposition 8.1.1, $\Lambda = \frac{p^2}{\pi^{(p-1)(i+j)}} e_0$ is a generating integral for H. Thus, by Proposition 4.3.4, $\alpha_m \cdot \Lambda \in H$ for $m = 1, \ldots, p^2$. Let $d_m = \alpha_m \cdot \Lambda$. Then

$$d_m = \sum_{a(p-1)+b=1}^{p^2-p} \frac{p^2 r_{l,m}}{\pi^{(p-1)(i+j)}} \left(\frac{1}{\pi^{ae'}} \sum_{\eta=0}^{a} \binom{a}{\eta} (-1)^{\eta} e_{(a-\eta)p} \right) \left(\frac{1}{\pi^{bi'}} \sum_{\iota=0}^{b} \binom{b}{\iota} (-1)^{\iota} e_{b-\iota} \right)$$
$$+ \sum_{\iota=c}^{p^2} \frac{p^2 r_{\iota,m}}{\pi^{(p-1)(i+j)}} \left(\frac{1}{\pi^{(\iota-c)e'}} \sum_{\eta=0}^{\iota-c} \binom{\iota-c}{\eta} (-1)^{\eta} e_{(\iota-c-\eta)p} \right),$$

where $c = p^2 - p + 1$.

We have $H(j') \subseteq H^*$, so that $H(j', 0) \subseteq H^*$ and $H \subseteq H(j', 0)^*$. By Proposition 8.1.1, $\varrho = \frac{p^2}{\pi^{(p-1)(e'+j)}} e_0$ is a generating integral for $H(j', 0)^*$, and so, by Proposition 4.3.4, a basis for $H(j', 0)^*$ can be written as

$$\left\{ \left(\frac{\gamma^p - 1}{\pi^{j'}} \right)^a \left(\frac{\gamma - 1}{\pi^0} \right)^b \cdot \varrho \right\} = \left\{ \frac{p^2}{\pi^{(p-1)(e'+j)}} A_a B_b \right\}, \tag{8.3}$$

where

$$A_a = \frac{1}{\pi^{aj'}} \sum_{\eta=0}^{a} \binom{a}{\eta} (-1)^{\eta} e_{(a-\eta)p}$$

and

$$B_b = \sum_{\iota=0}^{b} \binom{b}{\iota} (-1)^{\iota} e_{b-\iota}$$

for $0 \le a, b \le p-1$.

Now, since $d_m \in H \subseteq H(j', 0)^*$, d_m can be written as an integral linear combination of the basis (8.3) for $H(j', 0)^*$. Let m be such that $1 \le m \le p^2 - p$. Each term of d_m can be written as

$$\frac{p^2 r_{l,m}}{\pi^{(p-1)(i+j)}}\left(\frac{1}{\pi^{ae'}}\sum_{\eta=0}^{a}\binom{a}{\eta}(-1)^{\eta}e_{(a-\eta)p}\right)\left(\frac{1}{\pi^{bi'}}\sum_{\iota=0}^{b}\binom{b}{\iota}(-1)^{\iota}e_{b-\iota}\right)$$
$$= \frac{r_{l,m}\pi^{aj'}\pi^{e}}{\pi^{(p-1)i}\pi^{bi'}\pi^{ae'}}\left(\frac{p^2}{\pi^{(p-1)(e'+j)}}A_a B_b\right),$$

and so $\frac{r_{l,m}\pi^{aj'}\pi^{e}}{\pi^{(p-1)i}\pi^{bi'}\pi^{ae'}} \in R$ or

$$\begin{aligned}\operatorname{ord}(r_{l,m}\pi^{aj'}\pi^{e}) &\geq \operatorname{ord}(\pi^{(p-1)i}\pi^{bi'}\pi^{ae'}),\\ \operatorname{ord}(r_{l,m}) + aj' + e &\geq (p-1)i + bi' + ae',\\ \operatorname{ord}(r_{l,m}) &\geq aj + bi' - (p-1)i'.\end{aligned}$$ □

We can now show that the valuation condition holds in the case $i \geq e/p$.

Lemma 8.1.2. *Let H be an R-Hopf order in KC_{p^2} that induces the short exact sequence (8.2). If $i \geq e/p$, then $pi' \leq j'$.*

Proof. Let $\{a_m\}_{m=1}^{p^2}$ denote the R-basis for H^* as constructed in Lemma 8.1.1. Let $\overline{\alpha_m}$ denote the image of α_m under the R-module surjection $H^* \overset{\gamma^p\mapsto 1}{\rightarrow} H(i')$. Since $\{\overline{\alpha_m}\}$ is an R-basis for $H(i')$, we can assume that $r_{1,m'} = 1$ for some m', $1 \leq m' \leq p^2$.

Since $H^* = S \oplus H(j')$ for some R-module S, Lemma 8.1.1(i) implies that $m' \leq p^2 - p$, and so, since M' is upper-triangular, we have $r_{l,m'} = 0$ for all $l \geq p^2 - p + 1$. Thus the basis element $\alpha_{m'} \in H^*$ has the form

$$\alpha_{m'} = \sum_{l=a(p-1)+b=1}^{p^2-p} r_{l,m'}h^a k^b = k + \sum_{l=a(p-1)+b=2}^{p^2-p} r_{l,m'}h^a k^b.$$

Thus, H^* contains the pth power

$$\alpha_{m'}^p = k^p + \sum_{l=a(p-1)+b=2}^{p^2-p} r_{l,m'}^p h^{ap}k^{bp} + \sum_{\mathcal{P}} pu_{\mathcal{P}} \prod_{l=a(p-1)+b=1}^{p^2-p} (r_{l,m'}h^a k^b)^{n_l},$$

where the second summation is over all partitions $\mathcal{P}$ of p that are in the form $p = \Sigma_{l=1}^{p^2-p} n_l$, $n_l \geq 0$, and $u_{\mathcal{P}}$ is a unit of R dependent on the partition $\mathcal{P}$.

We claim that

$$\sum_{\mathcal{P}} pu_{\mathcal{P}} \prod_{l=a(p-1)+b=1}^{p^2-p} \left(r_{l,m'}h^a k^b\right)^{n_l} \in H^*.$$

By Lemma 8.1.1(ii), $\mathrm{ord}(r_{l,m'}) \geq aj + bi' - (p-1)i'$, and so there exist elements $s_l \in R$ for which

$$r_{l,m'} = \frac{s_l \pi^{aj} \pi^{bi'}}{\pi^{(p-1)i'}}.$$

Thus

$$\begin{aligned}\sum_{\mathcal{P}} pu_{\mathcal{P}} \prod_{a(p-1)+b=1}^{p^2-p} (r_{l,m'} h^a k^b)^{n_l} &= \sum_{\mathcal{P}} pu_{\mathcal{P}} \prod_{a(p-1)+b=1}^{p^2-p} \left(\frac{s_l \pi^{aj} \pi^{bi'}}{\pi^{(p-1)i'}} h^a k^b\right)^{n_l} \\ &= \sum_{\mathcal{P}} \frac{pu_{\mathcal{P}}}{\pi^{p(p-1)i'}} \prod_{a(p-1)+b=1}^{p^2-p} s_l^{n_l} (\pi^{aj} h^a \pi^{bi'} k^b)^{n_l} \\ &= \sum_{\mathcal{P}} \frac{pu_{\mathcal{P}}}{\pi^{p(p-1)i'}} \prod_{a(p-1)+b=1}^{p^2-p} s_l^{n_l} \left(\frac{\gamma^p-1}{\pi^{j'}}\right)^{an_l} \left(\frac{\gamma-1}{\pi^0}\right)^{bn_l},\end{aligned}$$

which is in H^* since $i \geq e/p$ implies $e'/p \geq i'$, which in turn yields $\mathrm{ord}(p) = e \geq p(p-1)i'$. We conclude that

$$k^p + \sum_{l=a(p-1)+b=2}^{p^2-p} r_{l,m'}^p h^{ap} k^{bp} \in H^*,$$

and thus

$$\begin{aligned}&\left(\frac{\gamma-1}{\pi^{i'}}\right)^p + \sum_{a(p-1)+b=2}^{p^2-p} r_{l,m'}^p \left(\frac{\gamma^p-1}{\pi^{e'}}\right)^{ap} \left(\frac{\gamma-1}{\pi^{i'}}\right)^{bp} \\ &= \frac{\gamma^p-1}{\pi^{pi'}} + \frac{1}{\pi^{pi'}} \sum_{\iota=1}^{p} \binom{p}{\iota} (-1)^{\iota} \gamma^{p-\iota} \\ &\quad + \sum_{a(p-1)+b=2}^{p^2-p} \frac{s_l^p}{\pi^{p(p-1)i'}} \left(\left(\frac{\gamma^p-1}{\pi^{j'}}\right)^p\right)^a \left(\left(\frac{\gamma-1}{\pi^0}\right)^p\right)^b\end{aligned}$$

is in H^*.

Now $\pi^{-pi'} \Sigma_{\iota=1}^{p} \binom{p}{\iota} (-1)^{\iota} \gamma^{p-\iota} \in H^*$, and all of the terms in the second summation above with $l = a(p-1) + b \geq p$ are in H^*. Thus

$$\frac{\gamma^p-1}{\pi^{pi'}} + \sum_{b=2}^{p-1} \frac{s_l^p}{\pi^{p(p-1)i'}} ((\gamma-1)^p)^b \in H^*.$$

Since this quantity is in $K\hat{C}_{p^2} \cap H^* = H(j')$, and since $\left\{\left(\frac{\gamma^p-1}{\pi^{j'}}\right)^b\right\}$, $b=0,\ldots,p-1$, is an R-basis for $H(j')$, we conclude that $pi' \le j'$. □

We next consider the case $i < e/p$.

Lemma 8.1.3. *Let H be an R-Hopf order in KC_{p^2} that induces the short exact sequence (8.2). If $i < e/p$, then $j' \ge e/p$.*

Proof. Since $H(i)$ injects into H, the Larson order $H(i,0) \subseteq H$. Thus $H^* \subseteq H(i,0)^* = A\left(e', i', \zeta_{p^2}^{-1}\right) = R\left[\frac{\gamma^p-1}{\pi^{e'}}, \frac{\gamma u-1}{\pi^{i'}}\right]$. Note that $A\left(e', i', \zeta_{p^2}^{-1}\right)$ is not Larson since $i < e/p$ implies $i' > e'/p$. By Lemma 7.1.6, u is a unit in $R\left[\frac{\gamma^p-1}{\pi^{e'}}\right]$, and thus $A\left(e', i', \zeta_{p^2}^{-1}\right) = R\left[\frac{\gamma^p-1}{\pi^{e'}}, \frac{\gamma-u^{-1}}{\pi^{i'}}\right]$.

Let $h = \dfrac{\gamma^p-1}{\pi^{e'}}$, $k = \dfrac{\gamma-u^{-1}}{\pi^{i'}}$. Then

$$Y = \left(k, k^2, \ldots, k^{p-1}, hk, hk^2, \ldots, hk^{p-1}, \ldots, \right.$$
$$\left. h^{p-1}k, h^{p-1}k^2, \ldots, h^{p-1}k^{p-1}, 1, h, \ldots, h^{p-1}\right)$$

is an R-basis for $A(e', i', \zeta_{p^2}^{-1})$. Therefore an R-basis $\{\alpha_m\}$ for H^* is given by the matrix product

$$YM = \left(\alpha_1, \alpha_2, \ldots, \alpha_{p^2}\right),$$

where M is an upper-triangular $p^2 \times p^2$ matrix with entries $r_{l,m} \in R$.

The condition $i' > e'/p$ implies $pi' > e' \ge j'$, and so H^* is not a Larson order, yet it does contain a largest Larson order $A(\Xi(H^*))$. Thus H^* contains $\dfrac{\gamma-1}{\pi^t}$ for some $t \ge 0$. There exist elements $s_m \in R$ with

$$\frac{\gamma-1}{\pi^t} = \sum_{m=1}^{p^2} s_m \alpha_m,$$

and so there exist elements $q_l \in R$ for which

$$\frac{\gamma-1}{\pi^t} = \sum_{l=a(p-1)+b=1}^{p^2-p} q_l h^a k^b + \sum_{\iota=c}^{p^2} q_\iota h^{\iota-c}, \quad c = p^2-p+1.$$

One has $q_l = 0$ for $2 \le l \le p^2-p$, and so

$$\frac{\gamma-1}{\pi^t} = q_1 k + \sum_{\iota=c}^{p^2} q_\iota h^{\iota-c}, \quad c = p^2-p+1$$

$$= q_1 \frac{\gamma-1}{\pi^{i'}} + q_1 \frac{1-u^{-1}}{\pi^{i'}} + \sum_{\iota=c}^{p^2} q_\iota h^{\iota-c}, \quad c = p^2-p+1.$$

If $\text{ord}(q_1) > i'$, then $\frac{\gamma - 1}{\pi^{\iota}} \notin H^*$, and thus $\text{ord}(q_1) \le i'$. Moreover,

$$\sum_{\iota=c}^{p^2} q_\iota h^{\iota - c} \in H^* \cap KC_{p^2} = H(j'),$$

and so $q_1 \frac{1-u^{-1}}{\pi^{i'}} \in H(j')$. Consequently, $1 - u^{-1} \in H(j')$. Now, by Lemma 7.1.6, $\text{ord}(1 - \zeta_{p^2}) = e'/p \ge j$; that is, $j' \ge e/p$. □

We now show that H in KC_{p^2} satisfies the valuation condition for $n = 2$.

Proposition 8.1.2. *Let H be an R-Hopf order in KC_{p^2} that induces the short exact sequence of* (8.2)*. Then either $pj \le i$ or $pi' \le j'$.*

Proof. Suppose $i \ge e/p$. Then, by Lemma 8.1.2, $pj' \le i'$. On the other hand, if $i < e/p$, then $j' \ge e/p$ by Lemma 8.1.3, and thus Lemma 8.1.2 can be applied to the dual short exact sequence to obtain $pj \le i$. □

8.2 Some Cohomology

In this section, we give a review of cohomology of groups, which will be needed in the subsequent section.

Let C_m denote the cyclic group of order m, generated by τ, let G be an Abelian group, and let G^m denote the subgroup of G generated by $\{g^m : g \in G\}$. An **extension of** G **by** C_m is a short exact sequence of groups

$$E : 1 \to G \xrightarrow{i} G' \xrightarrow{s} C_m \to 1.$$

Two extensions E_1, E_2 are **equivalent** if there exists an isomorphism $G_1' \to G_2'$ such that the diagram

$$\begin{array}{ccccccccc} E_1 : 1 & \to & G & \to & G_1' & \to & C_m & \to & 1 \\ & & \| & & \downarrow & & \| & & \\ E_2 : 1 & \to & G & \to & G_2' & \to & C_m & \to & 1 \end{array} \tag{8.4}$$

commutes. Let $E(G, C_m)$ denote the collection of equivalence classes of extensions of G by C_m. In this section, we compute $E(G, C_m)$ following [Rot02, §10.3].

A **cocycle** is a function $f : C_m \times C_m \to G$ that satisfies the conditions

$$f(1, \tau^j) = f(\tau^i, 1) = 1 \tag{8.5}$$

and

$$f\left(\tau^i, \tau^j\right) f\left(\tau^{i+j}, \tau^k\right) = f\left(\tau^j, \tau^k\right) f\left(\tau^i, \tau^{j+k}\right) \tag{8.6}$$

for $i, j, k = 0, \ldots, m-1$.

Proposition 8.2.1. *The collection of cocycles, denoted by $C(G, C_m)$, is an Abelian group under the product*

$$(f * g)(\tau^i, \tau^j) = f(\tau^i, \tau^j)g(\tau^i, \tau^j),$$

with identity element $f(\tau^i, \tau^j) = 1$, for all i, j.

Proof. Exercise. □

We can identify a subgroup of $C(G, C_m)$ as follows. Let $h : C_m \to G$ be a function with $h(1) = 1$. Let $f_h : C_m \times C_m \to G$ be defined as

$$f_h(\tau^i, \tau^j) = h(\tau^i)(h(\tau^{i+j}))^{-1}h(\tau^j)$$

for $i, j = 0, \ldots, m-1$. Then it is routine to check that f_h is a cocycle. We write the cocycle f_h as ∂h and call it the **coboundary of** h. Let $B(G, C_m)$ denote the collection of coboundaries

$$B(G, C_m) = \{\partial h : \ h : C_m \to G, h(1) = 1\}.$$

Then $B(G, C_m)$ is a subgroup of $C(G, C_m)$.

Proposition 8.2.2. *The quotient group $C(G, C_m)/B(G, C_m)$ is in a* 1-1 *correspondence with the equivalence classes of extensions $E(G, C_m)$.*

Proof. Let f_1, f_2 be cocycles that satisfy the condition

$$f_1\left(\tau^i, \tau^j\right)\left(f_2(\tau^i, \tau^j)\right)^{-1} = \partial h\left(\tau^i, \tau^j\right) = h(\tau^i)\left(h(\tau^{i+j})\right)^{-1} h(\tau^j)$$

for some $\partial h \in B(G, C_m)$. Then

$$h(\tau^{i+j}) f_1(\tau^i, \tau^j) = h(\tau^i)h(\tau^j) f_2(\tau^i, \tau^j). \tag{8.7}$$

On the Cartesian product $G_1' = G \times C_m$, define a multiplication

$$(a, \tau^i) \cdot_{f_1} (b, \tau^j) = (ab f_1(\tau^i, \tau^j), \tau^{i+j}),$$

and on $G_2' = G \times C_m$ define a multiplication

$$(a, \tau^i) \cdot_{f_2} (b, \tau^j) = (ab f_2(\tau^i, \tau^j), \tau^{i+j}).$$

Then there exist extensions of groups

$$E_1 : \ 1 \to G \to G_1' \to C_m \to 1$$

and

$$E_2 : \ 1 \to G \to G_2' \to C_m \to 1.$$

We claim that E_1 and E_2 are equivalent. To this end, define a map $h : G_1' \to G_2'$ by the rule $h((a, \tau^i)) = (ah(\tau^i), \tau^i)$. Then

$$\begin{aligned} h((a, \tau^i) \cdot_{f_1} (b, \tau^j)) &= h((abf_1(\tau^i, \tau^j), \tau^{i+j})) \\ &= (abh(\tau^{i+j}) f_1(\tau^i, \tau^j), \tau^{i+j}) \\ &= (abh(\tau^i)h(\tau^j) f_2(\tau^i, \tau^j), \tau^{i+j}) \quad \text{by (8.7)} \\ &= (ah(\tau^i), \tau^i) \cdot_{f_2} (bh(\tau^j), \tau^j) \\ &= h((a, \tau^i)) \cdot_{f_2} h((b, \tau^j)), \end{aligned}$$

and so h is an isomorphism that makes the diagram (8.4) commute.

Consequently, there is a well-defined map

$$\Psi : C(G, C_m)/B(G, C_m) \to E(G, C_m),$$

where $\Psi(fB(G, C_m))$ is the equivalence class represented by

$$E : \ 1 \to G \to G' \to C_m \to 1,$$

where $G' = G \times C_m$ is endowed with the binary operation

$$(a, \tau^i) \cdot_f (b, \tau^j) = (abf(\tau^i, \tau^j), \tau^{i+j}). \tag{8.8}$$

Evidently, Ψ is a bijection. □

The values of a given cocycle $f : C_m \times C_m \to G$ can be arranged in an $m \times m$ matrix M_f whose i, jth entry is $f(\tau^i, \tau^j) = a_{i,j}$ for $i, j = 0, \ldots, m-1$. Note that the entries in the first row and first column are all 1 by cocycle property (8.5). Moreover, since the binary operation on $G \times C_m$ is Abelian,

$$(a, \tau^i) \cdot (b, \tau^j) = (b, \tau^j) \cdot (a, \tau^i),$$

and so

$$(abf(\tau^i, \tau^j), \tau^{i+j}) = (baf(\tau^j, \tau^i), \tau^{j+i}),$$

which implies that

$$f(\tau^i, \tau^j) = f(\tau^j, \tau^i)$$

for all $i, j = 0, \ldots, m-1$. Thus M_f is symmetric. We prove the following.

Proposition 8.2.3. *Let C_m denote the cyclic group of order m generated by τ, let G be an Abelian group, and let G^m denote the subgroup of G generated by $\{g^m : g \in G\}$. Then there is a group isomorphism*

$$\Phi : G/G^m \to C(G, C_m)/B(G, C_m)$$

defined as

$$\Phi(wG^m) = f_w B(G, C_m),$$

where $f_w : C_m \times C_m \to G$ *is the cocycle in* $C(G, C_m)$ *whose values are given by the matrix*

$$M_{f_w} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 & w \\ 1 & \cdots & 1 & w & w \\ \vdots & & \vdots & & \vdots \\ 1 & w & w & \cdots & w \end{pmatrix}.$$

Proof. We first show that Φ is well-defined on cosets of G/G^m. Suppose $w \in vG^m$. Then $wv^{-1} = g^m$ for some $g \in G$, and the cocycle $f_{wv^{-1}} : C_m \times C_m \to G$ satisfies $f_{wv^{-1}} = \partial h$, where $h : C_m \to G$ is defined by $h(\tau^i) = g^i$. Thus $f_{wv^{-1}} \in B(G, C_m)$, and so Φ is well-defined.

Now,

$$\begin{aligned} \Phi(vG^m wG^m) &= \Phi(vwG^m) \\ &= f_{vw} B(G, C_m) \\ &= f_v B(G, C_m) f_w B(G, C_m), \end{aligned}$$

and so Φ is a group homomorphism. Next, suppose that $\Phi(wG^m) = \Phi(vG^m)$. Then $f_{wv^{-1}} \in B(G, C_m)$. Thus there exists a function $h : C_m \to G$, $h(1) = 1$ for which $\partial h = f_{wv^{-1}}$. Thus $wv^{-1} = g^m$ for some $g \in G$, and so $wG^m = vG^m$, which shows that Φ is an injection.

To show that Φ is surjective, let $fB(G, C_m)$ be a coset in $C(G, C_m)/B(G, C_m)$. Assuming that this coset can be written in the form $f_w B(G, C_m)$ for some $w \in G$, we have $\Psi(wG^m) = fB(G, C_m)$, and so Φ is surjective. So the remainder of this proof will be concerned with proving that the coset $fB(G, C_m)$ can be written in this form.

We know that f has matrix

$$M_f = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & a_{1,1} & a_{1,2} & \cdots & a_{1,m-1} \\ 1 & a_{2,1} & a_{2,2} & \cdots & a_{2,m-1} \\ \vdots & \vdots & \vdots & & \vdots \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_{m-1,1} & a_{m-1,2} & \cdots & a_{m-1,m-1} \end{pmatrix}$$

for elements $a_{i,j} \in G$ with M_f symmetric. In the second row of M_f, let l be the smallest integer for which $a_{1,l} \neq 1$. Define a function $h : C_m \to G$ by

$$h(\tau^i) = \begin{cases} 1 & \text{for } i = 0, \ldots, l \\ a_{1,l} & \text{for } i = l+1, \ldots, m-1. \end{cases}$$

Then ∂h is a coboundary with matrix $M_{\partial h}$ whose first and second rows and columns, up to and including the codiagonal, have the form

$$M_{\partial h} = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & \cdots & 1 \\ 1 & 1 & \cdots & 1 & a_{1,l}^{-1} & 1 & \cdots & 1 & * \\ \vdots & \vdots & * & * & * & * & * & * & * \\ 1 & 1 & * & * & * & * & * & * & * \\ 1 & a_{1,l}^{-1} & * & * & * & * & * & * & * \\ 1 & 1 & * & * & * & * & * & * & * \\ \vdots & \vdots & * & * & * & * & * & * & * \\ \vdots & 1 & * & * & * & * & * & * & * \\ 1 & * & * & * & * & * & * & * & * \end{pmatrix}.$$

Here the entry $a_{1,l}^{-1}$ is in the $(1, l)$th and $(l, 1)$th places. It follows that f is congruent modulo $B(G, C_m)$ to a cocycle whose matrix is of the form

$$M_f = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 1 & 1 & \cdots & 1 & * \\ 1 & 1 & * & * & * & * & * \\ 1 & 1 & * & * & * & * & * \\ 1 & \vdots & * & * & * & * & * \\ \vdots & 1 & * & * & * & * & * \\ 1 & * & * & * & * & * & * \end{pmatrix}.$$

Consequently, we can assume, without loss of generality, that the matrix M_f of the cocycle f is in the form above.

By the cocycle condition (8.6),

$$f(\tau, \tau) f(\tau^2, \tau^k) = f(\tau, \tau^k) f(\tau, \tau^{1+k})$$

for k, $0 \leq k \leq m-1$. But $f(\tau, \tau) = f(\tau, \tau^k) = f(\tau, \tau^{1+k}) = 1$ for $1 \leq k \leq m-3$, and so

$$f(\tau^2, \tau^k) = 1$$

for $k = 1, \ldots, m-3$. Now, again by (8.6),

$$f(\tau^2, \tau) f(\tau^3, \tau^k) = f(\tau, \tau^k) f(\tau^2, \tau^{1+k})$$

for all k. But, as we have seen above, $f(\tau^2, \tau) = f(\tau^2, \tau^k) = f(\tau^2, \tau^{1+k}) = 1$ for $1 \le k \le m-4$. Thus

$$f(\tau^3, \tau^k) = 1$$

for $k = 1, \dots, m-4$. Continuing in this manner, we see that

$$f(\tau^{m-2}, \tau^k) = 1$$

for $k = 1, \dots, m-(m-2+1) = 1$. It follows that the matrix for f is of the form

$$M_f = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 1 & \cdots & 1 & * \\ 1 & 1 & \cdots & 1 & * & * \\ 1 & \vdots & & * & * & * \\ \vdots & 1 & * & * & * & * \\ 1 & * & * & * & * & * \end{pmatrix}.$$

But what about the matrix entries below the main codiagonal? We show that they are all equal. By (8.6),

$$f(\tau, \tau) f(\tau^2, \tau^{m-1}) = f(\tau, 1) f(\tau, \tau^{m-1}).$$

But, as we have seen, this implies that

$$f(\tau^2, \tau^{m-1}) = f(\tau, \tau^{m-1}).$$

Moreover,

$$f(\tau, \tau^2) f(\tau^3, \tau^{m-1}) = f(\tau, \tau) f(\tau^2, \tau^{m-1}),$$

and so

$$f(\tau^3, \tau^{m-1}) = f(\tau^2, \tau^{m-1}).$$

Hence

$$f(\tau^{k+1}, \tau^{m-1}) = f(\tau^k, \tau^{m-1})$$

for $k = 1, \dots, m-2$. By (8.6),

$$f(\tau, \tau^k) f(\tau^{k+1}, \tau^{m-2}) = f(\tau, \tau^{m-2+k}) f(\tau^k, \tau^{m-2})$$

for all k. Since $f(\tau, \tau^k) = f(\tau, \tau^{m-2+k}) = 1$ for $k = 2, \dots, m-2$,

$$f(\tau^{k+1}, \tau^{m-2}) = f(\tau^k, \tau^{m-2})$$

for $k = 2, \dots, m-2$. Continuing in this manner, we see that the entries below the main codiagonal in a column are equal.

We next show that all of the entries below the main codiagonal are equal to a common value. By (8.6),

$$f(\tau,\tau)f(\tau^2,\tau^{m-2}) = f(\tau,\tau^{m-1})f(\tau,\tau^{m-2})$$

for all k, and thus

$$f(\tau^2,\tau^{m-2}) = f(\tau,\tau^{m-1}).$$

By (8.6),

$$f(\tau,\tau^2)f(\tau^3,\tau^{m-3}) = f(\tau,\tau^{m-1})f(\tau^2,\tau^{m-3}),$$

and thus

$$f(\tau^3,\tau^{m-3}) = f(\tau,\tau^{m-1}).$$

Continuing in this manner, we conclude that

$$f(\tau^k,\tau^{m-k}) = f(\tau,\tau^{m-1})$$

for $k = 2,\ldots,m-1$. Now

$$f(\tau^i,\tau^j) = f(\tau^l,\tau^k)$$

for all $i+j > m-1$, $l+k > m-1$, and so all of the entries below the main codiagonal are equal to a common value, say w. Thus the matrix of f is in the form

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 & w \\ 1 & \cdots & 1 & w & w \\ \vdots & & \vdots & & \vdots \\ 1 & w & w & \cdots & w \end{pmatrix}.$$

This completes the proof of the proposition. □

We summarize with the following proposition.

Proposition 8.2.4. *There is a* 1-1 *correspondence between the group G/G^m and the equivalence classes in $E(G,C_m)$. Specifically, a coset $wG^m \in G/G^m$ corresponds to an equivalence class of extensions represented by*

$$E_w : 1 \to G \to G'_w \to C_m \to 1,$$

where the group operation on the set $G'_w = G \times C_m$ is given as

$$(a,\tau^i)\cdot(b,\tau^j) = \begin{cases} (ab,\tau^{i+j}) & \text{if } i+j < m \\ (abw,\tau^{i+j-m}) & \text{if } i+j \geq m. \end{cases}$$

Proof. By Proposition 8.2.3 and Proposition 8.2.2, there exists a 1-1 correspondence $G/G^m \to E(G, C_m)$, where the coset wG^m corresponds to the matrix M_{f_w}. The definition of the binary operation follows from (8.8). □

8.3 Greither Orders

In this section, we compute the algebraic structure of the Hopf order H in the short exact sequence (8.2) assuming that $i \geq pj$, following closely the work of C. Greither [Gr92].

We shall employ the cohomology of the previous section in the following context. Let i, j be integers with $0 \leq i, j \leq e'$, and $pj \leq i$. Let $\mathbb{D}_i$ be the R-group scheme represented by the Larson order

$$H(i) = R\left[\frac{\tau - 1}{\pi^i}\right], \quad \langle\tau\rangle = C_p,$$

and let $\mathbb{E}_j$ denote the functor represented by the polynomial algebra

$$R\left[\frac{X-1}{\pi^j}, X^{-1}\right],$$

where X is indeterminate.

Proposition 8.3.1. *The R-algebra $R\left[\frac{X-1}{\pi^j}, X^{-1}\right]$ is an R-Hopf algebra with comultiplication, counit, and coinverse maps induced from the corresponding maps of the K-Hopf algebra $K[X, X^{-1}]$. Consequently, $\mathbb{E}_j$ is an R-group scheme that over K appears as $\mathbf{G}_{m,K} = \mathrm{Hom}_{K\text{-alg}}(K[X, X^{-1}], -)$.*

Proof. One readily computes

$$\Delta_{K[X,X^{-1}]}\left(\frac{X-1}{\pi^j}\right) = \frac{X-1}{\pi^j} \otimes 1 + 1 \otimes \frac{X-1}{\pi^j} + (X-1) \otimes \frac{X-1}{\pi^j}$$

and $\Delta_{K[X,X^{-1}]}(X^{-1}) = X^{-1} \times X^{-1}$. Moreover,

$$\epsilon_{K(X,X^{-1}]}\left(R\left[\frac{X-1}{\pi^j}, X^{-1}\right]\right) \subseteq R$$

and

$$\sigma_{K[X,X^{-1}]}\left(R\left[\frac{X-1}{\pi^j}, X^{-1}\right]\right) \subseteq R\left[\frac{X-1}{\pi^j}, X^{-1}\right]$$

since $X, \frac{X^{-1}-1}{\pi^j} \in R\left[\frac{X-1}{\pi^j}, X^{-1}\right]$. □

Observe that $\mathbb{E}_j(R) = U_j(R)$. An **extension of** $\mathbb{E}_j$ **by** $\mathbb{D}_i$ is a short exact sequence of group schemes

$$E:\ 1 \to \mathbb{E}_j \xrightarrow{i} G \xrightarrow{s} \mathbb{D}_i \to 1;$$

that is, an extension of $\mathbb{E}_j$ by $\mathbb{D}_i$ is a sequence as above in which $\mathbb{D}_i$ is the quotient sheaf of G by $\mathbb{E}_j$ (see Definition 3.3.3).

Observe that if E is an extension of $\mathbb{E}_j$ by $\mathbb{D}_i$, then it is not obvious that

$$E(S):\ 1 \to \mathbb{E}_j(S) \xrightarrow{i_S} G(S) \xrightarrow{s_S} \mathbb{D}_i(S) \to 1$$

is a short exact sequence of groups for an R-algebra S. M. Demazure and P. Gabriel [DG70, III, §6, 2.5] have provided the following proposition.

Proposition 8.3.2. *Let i, j be integers that satisfy $0 \le i \le e'$, $0 \le j \le pe'$. Then*

$$E:\ 1 \to \mathbb{E}_j \xrightarrow{i} G \xrightarrow{s} \mathbb{D}_i \to 1$$

is an extension of $\mathbb{E}_j$ by $\mathbb{D}_i$ if and only if

$$E(S):\ 1 \to \mathbb{E}_j(S) \xrightarrow{i_S} G(S) \xrightarrow{s_S} \mathbb{D}_i(S) \to 1$$

is an extension of $\mathbb{E}_j(S)$ by $\mathbb{D}_i(S)$ in the sense of §8.2 for each R-algebra S.

In view of Proposition 8.3.2, two extensions, E_1, and E_2 such are **equivalent** if there exists an isomorphism of group schemes $G_1 \to G_2$ such that the diagram

$$\begin{array}{ccccccccc} E_1(S): 1 & \to & \mathbb{E}_j(S) & \to & G_1(S) & \to & \mathbb{D}_i(S) & \to & 1 \\ & & \| & & \downarrow & & \| & & \\ E_2(S): 1 & \to & \mathbb{E}_j(S) & \to & G_2(S) & \to & \mathbb{D}_i(S) & \to & 1 \end{array}$$

commutes for each R-algebra S.

Let $E(\mathbb{E}_j, \mathbb{D}_i)$ denote the collection of equivalence classes of extensions of $\mathbb{E}_j$ by $\mathbb{D}_i$. We seek to compute $E(\mathbb{E}_j, \mathbb{D}_i)$.

In view of the cohomology already discussed, we should consider "cocycles modulo coboundaries." But what plays the role of the cocycles $C(G, C_m)$? Let $\mathbb{D}_i \times \mathbb{D}_i$ denote the product of group schemes. Then, by Proposition 2.4.2, the representing algebra of $\mathbb{D}_i \times \mathbb{D}_i$ is $H(i) \otimes_R H(i)$.

Definition 8.3.1. The natural transformation $f : \mathbb{D}_i \times \mathbb{D}_i \to \mathbb{E}_j$ is a **cocycle** if, for each R-algebra S and $x, y, z \in \mathbb{D}_i(S)$

$$f_S(x, y)(X) f_S(xy, z)(X) = f_S(y, z)(X) f_S(x, yz)(X),$$
$$f_S(x, 1)(X) = f_S(1, y)(X) = 1.$$

The collection of cocycles is denoted by $C(\mathbb{E}_j, \mathbb{D}_i)$.

Analogous to Proposition 8.2.1, $C(\mathbb{E}_j, \mathbb{D}_i)$ is a group under the binary operation

$$(f_S * g_S)(x, y)(X) = f_S(x, y)(X) g_S(x, y)(X)$$

for each R-algebra S, $x, y \in \mathbb{D}_i(S)$.

We seek to characterize these cocycles in terms of the cocycles we've already developed. By Yoneda's Lemma, $f \in C(\mathbb{E}_j, \mathbb{D}_i)$ corresponds to an R-algebra homomorphism,

$$\phi_f : R\left[\frac{X-1}{\pi^j}, X^{-1}\right] \to H(i) \otimes_R H(i),$$

that is determined by the two conditions

$$X \mapsto \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} a_{m,n}(e_m \otimes e_n) \in U(H(i) \otimes H(i))$$

and

$$\frac{\left(\sum_{m=0}^{p-1} \sum_{n=0}^{p-1} a_{m,n}(e_m \otimes e_n)\right) - 1}{\pi^j} \in H(i) \otimes H(i).$$

There is an injection

$$\iota : H(i) \otimes_R H(i) \to \bigoplus_{m=0}^{p-1} Re_m \otimes_R \bigoplus_{n=0}^{p-1} Re_n,$$

and the map $\iota\phi_f$ is an R-algebra homomorphism

$$\iota\phi_f : R\left[\frac{X-1}{\pi^j}, X^{-1}\right] \to \bigoplus_{m=0}^{p-1} Re_m \otimes_R \bigoplus_{m=0}^{p-1} Re_m = RC_p^* \otimes_R RC_p^*.$$

Consequently, the algebra homomorphism $\iota\phi_f$ corresponds to a natural transformation

$$\tilde{f} : \mathrm{Hom}_{R\text{-alg}}(RC_p^* \otimes_R RC_p^*, -) \to \mathbb{E}_j.$$

By Proposition 4.1.8, $\mathrm{Hom}_{R\text{-alg}}(RC_p^* \otimes_R RC_p^*, R) = C_p \times C_p$, and so

$$\tilde{f}_R : C_p \times C_p \to \mathbb{E}_j(R) = U_j(R).$$

Note that

$$\begin{aligned}\tilde{f}_R(\tau^m, \tau^n)(X) &= (\tau^m, \tau^n)(\iota\phi_f)(X)\\ &= (\tau^m, \tau^n)\left(\sum_{m'=0}^{p-1}\sum_{n'=0}^{p-1} a_{m',n'}(e_{m'} \otimes e_{n'})\right)\\ &= a_{m,n}.\end{aligned}$$

In this manner, f gives rise to a function

$$\hat{f} : C_p \times C_p \to U_j(R),$$

defined as $(\tau^m, \tau^n) \mapsto a_{m,n}$.

We can now prove the following proposition.

Proposition 8.3.3. *The natural transformation* $f : \mathbb{D}_i \times \mathbb{D}_i \to \mathbb{E}_j$ *is a cocycle in* $C(\mathbb{E}_j, \mathbb{D}_i)$ *if and only if* $\hat{f}$ *is a cocycle in* $C(U_j(R), C_p)$.

Proof. Suppose that the natural transformation $f : \mathbb{D}_i \times \mathbb{D}_i \to \mathbb{E}_j$ is a cocycle with algebra homomorphism ϕ_f. Then, for all $x, y, z \in \mathbb{D}_i(R)$,

$$f_R(x, y)(X) f_R(xy, z)(X) = f_R(y, z)(X) f_R(x, yz)(X).$$

Consequently, for all l, m, $0 \le l, m \le p - 1$,

$$\tilde{f}_R(\tau^l, \tau^m)(X)\tilde{f}_R(\tau^{l+m}, \tau^n)(X) = \tilde{f}_R(\tau^m, \tau^n)\tilde{f}_R(\tau^l, \tau^{m+n})(X),$$

so that

$$a_{l,m}a_{l+m,n} = a_{m,n}a_{l,m+n},$$

where $m + n$ and $l + m$ are taken modulo p. Thus

$$\hat{f}(\tau^l, \tau^m)\hat{f}(\tau^{l+m}, \tau^n) = \hat{f}(\tau^m, \tau^n)\hat{f}(\tau^l, \tau^{m+n}),$$

and hence $\hat{f}$ satisfies cocycle condition (8.6).

Moreover, since $f : \mathbb{D}_i \times \mathbb{D}_i \to \mathbb{E}_j$ is a cocycle,

$$f_R(x, 1)(X) = 1 = f_R(1, y)(X)$$

for all $x, y \in \mathbb{D}_i(R)$. Thus, for all $0 \le l, m \le p - 1$,

$$\tilde{f}_R(\tau^l, 1)(X) = 1 = \tilde{f}_R(1, \tau^m)(X),$$

so that

$$a_{l,0} = 1 = a_{0,m}$$

for all $0 \le l, m \le p-1$. Thus $\hat{f}$ satisfies the cocycle condition (8.5). It follows that $\hat{f}$ is in $C(G, C_m)$ with $G = U_j(R)$, $C_m = C_p$.

Now suppose that $\hat{f} : C_p \times C_p \to U_j(R)$ is a cocycle obtained from the natural transformation $f : \mathbb{D}_i \times \mathbb{D}_i \to \mathbb{E}_j$. Then, for all l, m, n, $0 \le l, m, n \le p-1$, one has

$$a_{l,m}a_{l+m,n} = a_{l,m+n}a_{m,n},$$

where $m+n$ and $l+m$ are taken modulo p. Thus,

$$\sum_{l=0}^{p-1}\sum_{m=0}^{p-1}\sum_{n=0}^{p-1} a_{l,m}a_{l+m,n}(e_l \otimes e_m \otimes e_n) = \sum_{l=0}^{p-1}\sum_{m=0}^{p-1}\sum_{n=0}^{p-1} a_{l,m+n}a_{m,n}(e_l \otimes e_m \otimes e_n),$$

which yields

$$\left(\sum_{l=0}^{p-1}\sum_{m=0}^{p-1} a_{l,m}(e_l \otimes e_m \otimes 1)\right)\left(\sum_{k=0}^{p-1}\sum_{n=0}^{p-1} a_{k,n}(\Delta(e_k) \otimes e_n)\right)$$
$$= \left(\sum_{m=0}^{p-1}\sum_{n=0}^{p-1} a_{m,n}(1 \otimes e_m \otimes e_n)\right)\left(\sum_{l=0}^{p-1}\sum_{k=0}^{p-1} a_{l,k}(e_l \otimes \Delta(e_k))\right).$$

Thus, for $x, y, z \in \mathbb{D}_i(S)$,

$$(x \otimes y \otimes z)\left(\sum_{l=0}^{p-1}\sum_{m=0}^{p-1} a_{l,m}(e_l \otimes e_m \otimes 1)\right)(x \otimes y \otimes z)\left(\sum_{k=0}^{p-1}\sum_{n=0}^{p-1} a_{k,n}(\Delta(e_k) \otimes e_n)\right)$$
$$= (x \otimes y \otimes z)\left(\sum_{m=0}^{p-1}\sum_{n=0}^{p-1} a_{m,n}(1 \otimes e_m \otimes e_n)\right)(x \otimes y \otimes z)\left(\sum_{l=0}^{p-1}\sum_{k=0}^{p-1} a_{l,k}(e_l \otimes \Delta(e_k))\right),$$

which implies

$$(x, y)\phi_f(X)(xy, z)\phi_f(X) = (y, z)\phi_f(X)(x, yz)\phi_f(X).$$

Thus

$$f_S(x, y)(X) f_S(xy, z)(X) = f_S(y, z)(X) f_S(x, yz)(X).$$

Now, assume the condition $1 = a_{m,0}$ for $m = 0, \ldots, p-1$, and let $x \in \mathbb{D}_i(S)$. Then

$$\begin{aligned}
1 &= x\left(\sum_{m=0}^{p-1} a_{m,0} e_m\right) \\
&= (x \otimes \lambda_S \epsilon_{H(i)})\left(\sum_{m=0}^{p-1}\sum_{n=0}^{p-1} a_{m,n}(e_m \otimes e_n)\right) \\
&= (x, 1)\phi_f(X) \\
&= f_S(x, 1)(X).
\end{aligned}$$

In a similar manner, the condition $1 = a_{0,n}$, for $n = 0, \ldots, p-1$, yields $f_S(1, y)(X) = 1$ for $y \in \mathbb{D}_i(S)$. Consequently, f is a cocycle. □

We identify the group $C(\mathbb{E}_j, \mathbb{D}_i)$ with the subgroup C of $C(U_j(R), C_p)$ defined as

$$C = \{g \in C(U_j(R), C_p) : \ g = \hat{f} \text{ for some } f \in C(\mathbb{E}_j, \mathbb{D}_i)\}.$$

We next consider coboundaries. Let $h : \mathbb{D}_i \to \mathbb{E}_j$ be a natural transformation that satisfies $h_S(1) = 1, \forall S$. Let $f_h : \mathbb{D}_i \times \mathbb{D}_i \to \mathbb{E}_j$ be the natural transformation defined as

$$(f_h)_S(x, y)(X) = h_S(x)(X)(h_S(xy))^{-1}(X)h_S(y)(X).$$

Then f_h satisfies the cocycle conditions of Definition 8.3.1. We denote this cocycle by ∂h. The collection of all cocycles of the form

$$\{\partial h : \ h : \mathbb{D}_i \to \mathbb{E}_j \text{ is a natural transformation}, h_S(1) = 1, \forall S\}$$

is a subgroup of $C(\mathbb{E}_j, \mathbb{D}_i)$ denoted by $B(\mathbb{E}_j, \mathbb{D}_i)$. $B(\mathbb{E}_j, \mathbb{D}_i)$ is the collection of **coboundaries**.

Observe that the hat operation on cocycles can be applied to the natural transformation $h : \mathbb{D}_i \to \mathbb{E}_j$. By Yoneda's Lemma, h corresponds to an R-algebra homomorphism,

$$\phi_h : R\left[\frac{X-1}{\pi^j}, X^{-1}\right] \to H(i),$$

which is determined by the conditions

$$X \mapsto \sum_{m=0}^{p-1} a_m e_m \in U(H(i))$$

and

$$\frac{(\sum_{m=0}^{p-1} a_m e_m) - 1}{\pi^j} \in H(i).$$

There is an injection

$$\iota : H(i) \to \bigoplus_{m=0}^{p-1} Re_m,$$

and the map $\iota\phi_h$ is an R-algebra homomorphism

$$\iota\phi_h : R\left[\frac{X-1}{\pi^j}, X^{-1}\right] \to \bigoplus_{m=0}^{p-1} Re_m = RC_p^*$$

that corresponds to a natural transformation

$$\tilde{h} : \mathrm{Hom}_{R\text{-alg}}(RC_p^*, -) \to \mathbb{E}_j$$

with

$$\tilde{h}_R : \mathrm{Hom}_{R\text{-alg}}(RC_p^*, R) = C_p \to \mathbb{E}_j(R) = U_j(R).$$

Note that

$$\begin{aligned} \tilde{h}_R(\tau^m)(X) &= (\tau^m)(\iota\phi_h)(X) \\ &= (\tau^m)\left(\sum_{m'=0}^{p-1} a_{m'} e_{m'}\right) \\ &= a_m. \end{aligned}$$

In this manner, h gives rise to a function

$$\hat{h} : C_p \to U_j(R),$$

defined as $\tau^m \mapsto a_m$.

One can compute the coboundary of $\hat{h}$ (as defined in §8.2) to obtain $\partial\hat{h}$, which is in $B(U_j(R), C_p)$.

Proposition 8.3.4. *The cocycle $f : \mathbb{D}_i \times \mathbb{D}_i \to \mathbb{E}_j$ is a coboundary ($f = \partial h$, for some h) if and only if the cocycle $\hat{f}$ is a coboundary ($\hat{f} = \partial\hat{h}$).*

Proof. Let $h : \mathbb{D}_i \to \mathbb{E}_j$ be a natural transformation with algebra map $\phi_h : R\left[\frac{X-1}{\pi^j}, X^{-1}\right] \to H(i)$ given by $X \mapsto \sum_{m=0}^{p-1} a_m e_m \in U(H(i))$, $\sum_{m=0}^{p-1} a_m e_m \in 1 + \pi^j H(i)$.

Let $f \in C(\mathbb{E}_j, \mathbb{D}_i)$ be a cocycle that satisfies

$$f_R(x, y)(X) = h_R(x)(X)(h_R(xy)(X))^{-1}h_R(y)(X)$$

for all $x, y \in \mathbb{D}_i(R)$. Then, for $0 \leq m, n \leq p-1$,

$$\tilde{f}_R(\tau^m, \tau^n)(X) = \tilde{h}_R(\tau^m)(X)(\tilde{h}_R(\tau^{m+n})(X))^{-1}\tilde{h}_R(\tau^n)(X).$$

Thus

$$a_{m,n} = a_m(a_{m+n})^{-1}a_m$$

for all $0 \leq m, n \leq p-1$ ($m+n$ taken modulo p), and so $\hat{f} = \partial\hat{h}$.

Now suppose $\partial\hat{h} = \hat{f}$; that is, suppose that

$$a_{m,n} = a_m(a_{m+n})^{-1}a_n$$

for $0 \leq m, n \leq p-1$ ($m+n$ taken modulo p). Then

$$\begin{aligned}
\sum_{m,n=0}^{p-1} a_{m,n}(e_m \otimes e_n) &= \sum_{m,n=0}^{p-1} a_m(a_{m+n})^{-1}a_n(e_m \otimes e_n) \\
&= \sum_{m=0}^{p-1} a_m \sum_{n=0}^{p-1} a_n \sum_{k=0}^{p-1} a_k^{-1} \frac{1}{p} \sum_{l=0}^{p-1} \zeta_p^{-lk}(\zeta_p^{ml+nl})(e_m \otimes e_n) \\
&= \sum_{m=0}^{p-1} a_m \sum_{n=0}^{p-1} a_n \sum_{k=0}^{p-1} a_k^{-1} \frac{1}{p} \sum_{l=0}^{p-1} \zeta_p^{-lk}(\tau^l \otimes \tau^l)(e_m \otimes e_n) \\
&= \sum_{m=0}^{p-1} a_m(e_m \otimes 1) \sum_{k=0}^{p-1} a_k^{-1}\Delta_{H(i)}(e_k) \sum_{n=0}^{p-1} a_n(1 \otimes e_n).
\end{aligned} \tag{8.9}$$

Let ϕ_f denote the algebra map of f. Let $x, y \in \mathbb{D}_i(S)$. Then the relation (8.9) implies that

$$(x, y)\phi_f(X) = (x)\phi_h(X)((xy)\phi_h(X))^{-1}(y)\phi_h(X),$$

which yields

$$f_S(x, y)(X) = h_S(x)(X)(h_S(xy)(X))^{-1}h_S(y)(X),$$

and hence $\partial h = f$. □

By Proposition 8.3.4, we can identify the group $B(\mathbb{E}_j, \mathbb{D}_i)$, with the subgroup of $B(U_j(R), C_p)$ defined as

$$B = \{\partial k : k = \hat{h} \text{ for some } h : \mathbb{D}_i \to \mathbb{E}_j\}.$$

Analogous to Proposition 8.2.2, there is a bijection

$$\Psi : C/B \to E(\mathbb{E}_j, \mathbb{D}_i),$$

and through Ψ one can define a group operation on $E(\mathbb{E}_j, \mathbb{D}_i)$: for E_1, E_2, let

$$E_1 * E_2 = \Psi(xy),$$

where $\Psi(x) = E_1$ and $\Psi(y) = E_2$. Clearly, $E(\mathbb{E}_j, \mathbb{D}_i) \cong C/B$.

We want to characterize the quotient C/B.

Proposition 8.3.5. $C/B \cong U_{pi'+j}(R)/U_{i'+j}^p(R)$.

Proof. Let $\hat{f} \in C$. By §8.2, $\hat{f}$ has matrix

$$M_{\hat{f}} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & a_{1,1} & a_{1,2} & \cdots & a_{1,m-1} \\ 1 & a_{2,1} & a_{2,2} & \cdots & a_{2,m-1} \\ \vdots & \vdots & \vdots & & \vdots \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_{m-1,1} & a_{m-1,2} & \cdots & a_{m-1,m-1} \end{pmatrix}$$

for elements $a_{i,j} \in U_j(R)$ with $M_{\hat{f}}$ symmetric.

Since

$$\sum_{m=0}^{p-1}\sum_{n=0}^{p-1} a_{m,n}(e_m \otimes e_n) \in 1 + \pi^j (H(i) \otimes H(i)),$$

$$\left\langle (\gamma-1)^a \otimes (\gamma-1)^b, \sum_{m=0}^{p-1}\sum_{n=0}^{p-1} a_{m,n}(e_m \otimes e_n) \right\rangle \in \pi^{(a+b)i'} R$$

for $0 \leq a, b \leq p-1$, $a + b > 0$. In the second row of $M_{\hat{f}}$, let l be the smallest integer for which $a_{1,l} \neq 1$. Now,

$$\left\langle \gamma - 1 \otimes (\gamma-1)^l, \sum_{m=0}^{p-1}\sum_{n=0}^{p-1} a_{m,n}(e_m \otimes e_n) \right\rangle = 1 - a_{1,l} \in \pi^{(1+l)i'} R. \quad (8.10)$$

Consider the partial sum $\sum_{n=0}^{l} a_{1,n}e_n$. Then, by (8.10), this sum satisfies the first $l+2$ conditions for membership in $H(i)$ (see Lemma 7.1.6). By using Lemma 7.1.7, we can extend this sum to an element $y \in H(i)$.

The element y determines an R-algebra map

$$\phi_y : R\left[\frac{X-1}{\pi^j}, X^{-1}\right] \to H(i), \quad X \mapsto y,$$

which corresponds to a natural transformation $s = h_{\phi_y} : \mathbb{D}_i \to \mathbb{E}_j$ and a function

$$\hat{s} : C_p \to U_j(R).$$

Now $\partial\hat{s}$ is a cocycle in C, and $\hat{f} \cdot \partial\hat{s}$ has a matrix whose second row satisfies

$$a_{1,0} = a_{2,0} = \cdots = a_{1,l} = 1.$$

As in §8.2, we see that $\hat{f} \cdot \partial\hat{h} = f_w$ for some $\partial\hat{h} \in B$, where f_w has $p \times p$ matrix

$$M_w = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 & w \\ 1 & \cdots & 1 & w & w \\ \vdots & & \vdots & & \vdots \\ 1 & w & w & \cdots & w \end{pmatrix}$$

for $w \in U_j(R)$ and so each element $\hat{f} \in C$ is congruent modulo B to a cocycle in C of the form f_w.

Next, one shows that a cocycle f_w in $C(U_j(R), C_p)$ with matrix in the form M_w, $w \in U_j(R)$, corresponds to a cocycle in C if and only if $\mathrm{ord}(1-w) \geq pi' + j$; that is, if and only if $w \in U_{pi'+j}(R)$. Moreover, f_w is trivial in C if and only if $w \in U^p_{i'+j}(R)$. (See Greither's proof in [Gr92] for details.) It follows that $C/B \cong U_{pi'+j}(R)/U^p_{i'+j}(R)$. □

As a consequence of Proposition 8.3.5,

$$E(\mathbb{E}_j, \mathbb{D}_i) \cong U_{pi'+j}(R)/U^p_{i'+j}(R).$$

Let $E_{\text{gen-triv}}(\mathbb{E}_j, \mathbb{D}_i)$ denote the collection of **generically trivial** extensions; that is, those elements in $E(\mathbb{E}_j, \mathbb{D}_i)$ that over K appear as

$$1 \to \mathbf{G}_{m,K} \to \mathbf{G}_{m,K} \times \boldsymbol{\mu}_{p,K} \to \boldsymbol{\mu}_{p,K} \to 1.$$

Proposition 8.3.6. $E_{\text{gen-triv}}(\mathbb{E}_j, \mathbb{D}_i) \cong U_{i'+(j/p)}(R)/U_{i'+j}(R).$

Proof. Over K, one has an isomorphism

$$E(\mathbf{G}_{m,K}, \boldsymbol{\mu}_{p,K}) \cong K^\times/(K^\times)^p,$$

and so the generically trivial extensions correspond to units w that are pth roots in K. □

Let $\mathbb{D}_j = \mathrm{Hom}_{R\text{-alg}}(H(j), -)$ with $H(j) = R\left[\frac{\eta-1}{\pi^j}\right]$, $\eta^p = 1$, and let $E(\mathbb{D}_j, \mathbb{D}_i)$ denote the extensions of $\mathbb{D}_j$ by $\mathbb{D}_i$. Let $E_{\text{gen-triv}}(\mathbb{D}_j, \mathbb{D}_i)$ denote the collection of extensions that over K appear as

$$1 \to \boldsymbol{\mu}_{p,K} \to \boldsymbol{\mu}_{p,K} \times \boldsymbol{\mu}_{p,K} \to \boldsymbol{\mu}_{p,K} \to 1.$$

We want to replace $\mathbb{E}_j$ with $\mathbb{D}_j$ in Proposition 8.3.6 and compute $E_{\text{gen-triv}}(\mathbb{D}_j, \mathbb{D}_i)$. The group schemes $\mathbb{E}_j$ and $\mathbb{D}_i$ are related, and so this computation is possible. Let

$$\mathbf{G}'_{m,K} = \mathrm{Hom}_{K\text{-alg}}(K[Y, Y^{-1}], -),$$

with Y indeterminate, and let $\mathbb{E}_{pj} = \mathrm{Hom}_{R\text{-alg}}(R\left[\frac{Y-1}{\pi^{pj}}, Y^{-1}\right], -)$. Then there exists a short exact sequence of R-group schemes

$$1 \to \mathbb{D}_i \to \mathbb{E}_j \xrightarrow{p} \mathbb{E}_{pj} \to 1 \tag{8.11}$$

that is induced from the short exact sequence of K-group schemes

$$1 \to \boldsymbol{\mu}_{p,K} \to \mathbf{G}_{m,K} \xrightarrow{p} \mathbf{G}'_{m,K} \to 1$$

of §3.4.

We now state C. Greither's main result [Gr92, II, Corollary 3.6(b)].

Proposition 8.3.7. *(Greither) Let i, j be integers with $0 \le i, j \le e'$, $pj \le i$.*

(i) There is an isomorphism

$$E_{\text{gen}-\text{triv}}(\mathbb{D}_j, \mathbb{D}_i) \cong (U_{i'+(j/p)}(R) \cap U_{(i'/p)+j}(R))/U_{i'+j}(R),$$

where the coset $vU_{i'+j}(R)$ corresponds to an equivalence class of extensions represented by the extension

$$E_v : 1 \to \mathbb{D}_j \to G \to \mathbb{D}_i \to 1.$$

(ii) The extension E_v corresponds to a short exact sequence of R-Hopf orders

$$E'_v : R \to H(i) \to R\left[\frac{\tau-1}{\pi^i}, \frac{\eta a_{v^{-1}} - 1}{\pi^j}\right] \to H(j) \to R,$$

where $a_{v^{-1}} = \displaystyle\sum_{m=0}^{p-1} v^{-m} e_m$, where e_m are the minimal idempotents in $KC_p = K\langle\tau\rangle$. The middle term is an R-Hopf order in $K(C_p \times C_p)$.

Proof. Proof of (i). The short exact sequence (8.11) induces the exact sequence

$$1 \to E_{\text{gen-triv}}(\mathbb{D}_j, \mathbb{D}_i) \to E_{\text{gen-triv}}(\mathbb{E}_j, \mathbb{D}_i) \xrightarrow{p} E_{\text{gen-triv}}(\mathbb{E}_{pj}, \mathbb{D}_i).$$

Consequently,

$$E_{\text{gen-triv}}(\mathbb{D}_j, \mathbb{D}_i) = \ker\left(E_{\text{gen-triv}}(\mathbb{E}_j, \mathbb{D}_i) \xrightarrow{p} E_{\text{gen-triv}}(\mathbb{E}_{pj}, \mathbb{D}_i)\right).$$

Now, by Proposition 8.3.6,

$$E_{\text{gen-triv}}(\mathbb{E}_j, \mathbb{D}_i) \cong U_{i'+(j/p)}(R)/U_{i'+j}(R)$$

and

$$E_{\text{gen-triv}}(\mathbb{E}_{pj}, \mathbb{D}_i) \cong U_{i'+j}(R)/U_{i'+pj}(R),$$

from which (i) follows.

We next prove (ii). Let E_v be the generically trivial extension of $\mathbb{D}_j$ by $\mathbb{D}_j$ determined by the element $v \in U_{i'+(j/p)}(R) \cap U_{(i'/p)+j}(R)$. Then, over K, E_v appears as

$$\begin{aligned} E_{v,K} :\ 1 &\to \mathrm{Hom}_{K\text{-alg}}(H(j) \otimes_R K, -) \\ &\to \mathrm{Hom}_{K\text{-alg}}(H(j) \otimes_R K, -) \times \mathrm{Hom}_{K\text{-alg}}(H(i) \otimes_R K, -) \\ &\to \mathrm{Hom}_{\text{K-alg}}(H(i) \otimes_R K, -) \to 1. \end{aligned}$$

The group structure of

$$\mathrm{Hom}_{K\text{-alg}}(H(j) \otimes_R K, -) \times \mathrm{Hom}_{K\text{-alg}}(H(i) \otimes_R K, -)$$

is given by a cocycle $\hat{f} \in C$ whose matrix is M_{v^p}.

The extension $E_{v,K}$ is equivalent to the trivial extension

$$1 \to \boldsymbol{\mu}_{p,K} \to \boldsymbol{\mu}_{p,K} \times \boldsymbol{\mu}_{p,K} \to \boldsymbol{\mu}_{p,K} \to 1,$$

and so the natural transformation $h : \mathbb{D}_i \to \mathbb{E}_j$ given as $X \mapsto \sum_{m=0}^{p-1} v^m e_m$ determines a group scheme isomorphism

$$h : \mathrm{Hom}_{K\text{-alg}}((H(j) \otimes_R H(i)) \otimes_R K, -) \to \mathrm{Hom}_{K\text{-alg}}(K\langle\eta\rangle \otimes K\langle\tau\rangle, -),$$

defined as $h_S(x, y) = (xh_S(y), y)$, for a K-algebra S and $x \in \mathrm{Hom}_{K\text{-alg}}(H(j) \otimes_R K, S)$, $y \in \mathrm{Hom}_{K\text{-alg}}(H(i) \otimes_R K, S)$.

Note that $K\langle\eta\rangle \otimes K\langle\tau\rangle \cong K[\eta,\tau]$ and $(H(j) \otimes_R H(i)) \cong R\left[\frac{\eta-1}{\pi^j}, \frac{\tau-1}{\pi^i}\right]$. Thus the isomorphism h yields the K-algebra homomorphism

$$\varrho : K[\eta,\tau] \to K\left[\frac{\eta-1}{\pi^j}, \frac{\tau-1}{\pi^i}\right]$$

with $\varrho(\eta) = \eta a_{v^{-1}}$, $\varrho(\tau) = \tau$. Thus

$$\varrho\left(R\left[\frac{\eta-1}{\pi^j}, \frac{\tau-1}{\pi^i}\right]\right) = R\left[\frac{\tau-1}{\pi^i}, \frac{\eta a_{v^{-1}}-1}{\pi^j}\right],$$

which is the representing algebra of the group scheme G. Consequently, $R\left[\frac{\tau-1}{\pi^i}, \frac{\eta a_v-1}{\pi^j}\right]$ is an R-Hopf algebra.

We leave it to the reader to show that $R\left[\frac{\tau-1}{\pi^i}, \frac{\eta a_{v^{-1}}-1}{\pi^j}\right]$ is an R-Hopf order in $K(C_p \times C_p)$ that induces the short exact sequence

$$R \to H(i) \to R\left[\frac{\tau-1}{\pi^i}, \frac{\eta a_{v^{-1}}-1}{\pi^j}\right] \to H(j) \to R.$$

□

But how do we obtain Hopf orders in KC_{p^2} from the extensions of Proposition 8.3.7? The key is to endow the collection of short exact sequences of Hopf orders with a group product, which we describe as follows. Let

$$E^{(1)} : R \to H(i) \to H_1 \stackrel{s_1}{\to} H(j) \to R,$$

$$E^{(2)} : R \to H(i) \to H_2 \stackrel{s_2}{\to} H(j) \to R,$$

be short exact sequences of Hopf algebras. Recalling that the tensor product of two Hopf algebras is again a Hopf algebra, we obtain a short exact sequence of R-Hopf algebras,

$$R \to H(i) \otimes_R H(i) \to H_1 \otimes_R H_2 \stackrel{s_1 \otimes s_2}{\to} H(j) \otimes_R H(j) \to R.$$

There is a unique map ϕ that makes the following diagram commute:

$$\begin{array}{ccccccc}
 & & \mathrm{coker}(\Delta_{H(j)}) & = & \mathrm{coker}(\Delta_{H(j)}) & & \\
 & & \uparrow \phi & & \uparrow & & \\
R \to & H(i) \otimes_R H(i) \to & H_1 \otimes_R H_2 & \stackrel{s_1 \otimes s_2}{\to} & H(j) \otimes_R H(j) & \to R \\
\| & \| & \uparrow & & \uparrow \Delta_{H(j)} & \| \\
R \to & H(i) \otimes_R H(i) \to & \ker(\phi) & \to & H(j) & \to R
\end{array}$$

And there is a map ψ that makes the following diagram commute:

$$\begin{array}{ccccccccc} R & \to & H(i)\otimes_R H(i) & \to & \ker(\phi) & \to & H(j) & \to & R \\ \| & & \downarrow m & & \downarrow & & \| & & \| \\ R & \to & H(i) & \stackrel{\psi}{\to} & \ker(\phi)/\ker(m) & \to & H(j) & \to & R \end{array}$$

The short exact sequence in the bottom row is the **Baer product**

$$E = E^{(1)} * E^{(2)}.$$

The Baer product endows the collection of short exact sequences with the structure of a group.

Now, in our case, since $pj \le i$, there exists an extension of Larson orders

$$E_0: \ R \to H(i) \to R\left[\frac{\tau - 1}{\pi^i}, \frac{\eta - 1}{\pi^j}\right] \to H(j) \to R, \ \eta^p = \tau.$$

The Baer product $E_0 * E'_v$ is an extension

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

where $g = \eta$, $g^p = \eta^p = \tau$, whose middle term is an R-Hopf order in KC_{p^2} that we call a **Greither order**. A Greither order is determined by two valuation parameters i and j and one unit parameter $u = v^{-1}$, and will be denoted by $A(i, j, u)$.

Now suppose that H is an R-Hopf order in KC_{p^2}, that induces the short exact sequence

$$E : R \to H(i) \to H \to H(j) \to R,$$

where $pj \le i$. Then the Baer product $E_0^{-1} * E$ is a short exact sequence of the form

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

where H' is an R-Hopf order in $K(C_p \times C_p)$. There is a corresponding short exact sequence of R-group schemes

$$1 \to \mathbb{D}_j \to \mathrm{Hom}_{R\text{-alg}}(H', -) \to \mathbb{D}_i \to 1,$$

which is genericaly trivial. Now, by Proposition 8.3.7, $E_0^{-1} * E = E'_v$ for some $v \in U_{i'+(j/p)}(R) \cap U_{(i'/p)+j}(R)$. Thus $E = E_0 * E'_v$, and so, H is a Greither order.

Thus we have solved the problem that was stated at the beginning of this section: for $pj \le i$, the middle term in the short exact sequence

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

is a Greither order $A(i, j, u)$, where u represents a class in the quotient $(U_{i'+(j/p)}(R) \cap U_{(i'/p)+j}(R))/U_{i'+j}(R)$.

If $j' \geq pi'$, then Greither's result may be used to give the structure of H^*.

How does the collection of Greither orders relate to the Larson orders in KC_{p^2}? It is not too hard to prove the following.

Proposition 8.3.8. *Let $A(i, j, u)$ be a Greither order. Then $A(i, j, u)$ is the Larson order $H(i, j)$ in KC_{p^2} if and only if* $\text{ord}(1-u) \geq i' + j$.

Proof. Exercise. □

Not all Hopf orders in KC_{p^2} are Greither orders, however. For example, in the short exact sequence

$$R \to H(e') \to RC^*_{p^2} \to H(e') \to R,$$

one has $e' \not\geq pe'$.

But in view of the valuation condition (Proposition 8.1.2), a given R-Hopf order in KC_{p^2} is either of the form $A(i, j, u)$ or $A(i, j, u)^*$. So, to give a full account of the structure of Hopf orders in KC_{p^2}, one needs to obtain the algebraic structure of $A(i, j, u)^*$.

We need a lemma. Let $\langle g \rangle = C_{p^2}$, $\langle \gamma \rangle = \hat{C}_{p^2}$, and let $\langle\ ,\ \rangle :\ K\hat{C}_{p^2} \times KC_{p^2} \mapsto K$ denote the duality map.

Lemma 8.3.1. *Let e_i denote the minimal idempotents of KC_p, and let $\hat{e}_j$ denote the minimal idempotents of $K\hat{C}_p$. Then*

$$\langle \hat{e}_k \gamma^{pc+d}, e_j g^{pa+b} \rangle = \zeta_{p^2}^{(pa+b)(pc+d)}$$

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

Proof. Exercise. □

Proposition 8.3.9. *Assume that K contains ζ_{p^2}, and let*

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

be a Greither order in KC_{p^2}. Let $B = R\left[\frac{\gamma^p - 1}{\pi^{j'}}\right]$, and let

$$J = B\left[\frac{\gamma a_{\tilde{u}} - 1}{\pi^{i'}}\right],$$

where $\tilde{u} = \zeta_{p^2}^{-1} u^{-1}$, $a_{\tilde{u}} = \sum_{m=0}^{p-1} \tilde{u}^m \rho_m$, and $\rho_m = \frac{1}{p} \sum_{l=0}^{p-1} \zeta_p^{-m} \gamma^{pl}$. Then $J = A(i, j, u)^*$.

Proof. By Proposition 7.1.3, it suffices to show that

$$\langle J, A(i, j, u)\rangle \subseteq R,$$

and this is equivalent to the conditions

$$\langle \gamma^p - 1, (g^p - 1)^q (ga_u - 1)^r\rangle \in \pi^{qi+rj+j'} R \tag{8.12}$$

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

$$\langle \gamma a_{\tilde{u}} - 1, (g^p - 1)^q (ga_u - 1)^r\rangle \in \pi^{qi+rj+i'} R \tag{8.13}$$

for $q, r = 0, \ldots, p-1, q + r > 0$. One quickly sees that (8.12) is equivalent to $(\zeta_p - 1)^r \in \pi^{rj+j'} R$ for $r = 1, \ldots, p-1$, which holds.

To show that (8.13) holds, let $S = \langle \gamma a_{\tilde{u}} - 1, (g^p - 1)^q (ga_u - 1)^r\rangle$, let $\sum_{c,d=0}^{q,r}$ denote $\sum_{c=0}^{q}\sum_{d=0}^{r}$, and let $C(c,d) = \binom{q}{c}\binom{r}{d}(-1)^{q-c}(-1)^{r-d}$. Then

$$\begin{aligned}
S &= \sum_{c,d=0}^{q,r} C(c,d)\langle \gamma a_{\tilde{u}} - 1, g^{pc}(ga_u)^d\rangle \\
&= \sum_{c,d=0}^{q,r} C(c,d)\langle \gamma a_{\tilde{u}}, g^{pc}(ga_u)^d\rangle - \sum_{c,d=0}^{q,r} C(c,d)\langle 1, g^{pc}(ga_u)^d\rangle \\
&= \sum_{c,d=0}^{q,r} C(c,d)\langle \gamma a_{\tilde{u}}, g^{pc}(ga_u)^d\rangle - \sum_{c,d=0}^{q,r} C(c,d) \\
&= \sum_{c,d=0}^{q,r} C(c,d)\langle \gamma a_{\tilde{u}}, a_{u^d} g^{pc+d}\rangle - \sum_{c,d=0}^{q,r} C(c,d) \\
&= \sum_{c,d=0}^{q,r} C(c,d)\sum_{i,j} u^{di}\tilde{u}^j \langle \hat{e}_j\gamma, e_i g^{pc+d}\rangle - \sum_{c,d=0}^{q,r} C(c,d) \\
&= \sum_{c,d=0}^{q,r} C(c,d) u^d \tilde{u}^d \zeta_{p^2}^{pc+d} - \sum_{c,d=0}^{q,r} C(c,d) \quad \text{(by Lemma 8.3.1)} \\
&= \sum_{c,d=0}^{q,r} C(c,d)(u\tilde{u}\zeta_{p^2})^d \zeta_p^c - \sum_{c,d=0}^{q,r} C(c,d)
\end{aligned}$$

$$= \sum_{c,d=0}^{q,r} C(c,d)\zeta_p^c - \sum_{c,d=0}^{q,r} C(c,d) \quad \text{since } u\tilde{u}\zeta_{p^2} = 1$$

$$= \sum_{c,d=0}^{q,r} C(c,d)(\zeta_p^c - 1).$$

Now $S = 0$ unless $q \geq 1$, $r = 0$. In this case, $S = (\zeta_p - 1)^q$, which is in $\pi^{qi'+i}R$. Thus (8.13) holds. □

And so we have shown that an arbitrary R-Hopf order in KC_{p^2} can be written in the form $A(i, j, u)$ for some integers $0 \leq i, j \leq e'$ and unit $u \in R$.

The largest Larson order in $A(i, j, u)$ can be computed as follows.

Proposition 8.3.10. *Let $A(i, j, u)$ be an R-Hopf order in KC_{p^2}. Then*

$$H(i,l) = A(\Xi(A(i, j, u)))$$

is the Larson order $H(i,l)$, where $l = j$ if $\text{ord}(1 - u) \geq i' + j$ *and* $l = i - e' + \text{ord}(1 - u)$ *otherwise.*

Proof. If $\text{ord}(1 - u) \geq i' + j$, then $v = u^{-1}$ corresponds to the trivial class in $E_{\text{gen-triv}}(\mathbb{D}_j, \mathbb{D}_i)$. Thus, the Baer product $E_0 * E'_v = E_0$, which says that $A(i, j, u) = H(i, j)$. On the other hand, suppose that $\text{ord}(1 - u) < i' + j$. We have

$$\frac{ga_u - 1}{\pi^j} = g\left(\frac{a_u - 1}{\pi^j}\right) + \frac{g - 1}{\pi^j}.$$

Now, by Lemma 7.1.6, $l = \text{ord}(1 - u) - i'$ is the largest integer for which $\frac{a_u - 1}{\pi^l} \in H(i)$. Therefore l is the largest integer for which $\frac{g-1}{\pi^l} \in H(i)$. Thus, $A(\Xi(A(i, j, u))) = H(i,l)$. □

8.4 Hopf Orders in KC_4, KC_9

In this section, we present an alternate approach to proving the valuation condition (Proposition 8.1.2) for the cases $p = 2, 3$. We show that if

$$R \to H(i) \to H \xrightarrow{s} H(j) \to R$$

is a short exact sequence where H is a Hopf order in KC_4 or KC_9, then either $pj \leq i$ or $pi' \leq j'$.

We begin with a lemma.

Lemma 8.4.1. *Let H be an R-Hopf order in KC_{p^2}. Suppose H^* can be written in the form*

$$H^* = R\left[\frac{\gamma^p - 1}{\pi^{j'}}, \frac{\gamma u - 1}{\pi^{i'}}\right],$$

where $u = \sum_{m=0}^{p-1} b_m \eta_m \in K\hat{C}_p$ and where η_m are the minimal idempotents in $K\langle\gamma^p\rangle$. Then H is of the form

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

where $a_v = \sum_{m=0}^{p-1} v^m f_m$, $v = \zeta_{p^2}^{-1} b_1^{-1}$, and where f_m are the minimal idempotents in $K\langle g^p\rangle$.

Proof. Let $v = \zeta_{p^2}^{-1} b_1^{-1}$. We claim that

$$\left\langle \frac{g a_v - 1}{\pi^j}, H^* \right\rangle \subseteq R,$$

which is equivalent to

$$\operatorname{ord}\left(\langle g a_v - 1, (\gamma^p - 1)^r (\gamma u - 1)^s\rangle\right) \geq j + rj' + si' \tag{8.14}$$

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

$$\begin{aligned}\langle g a_v - 1, (\gamma^p - 1)^r (\gamma u - 1)^s\rangle &= (\zeta_p - 1)^r \sum_{q=0}^{s} \binom{s}{q} (-1)^{s-q} \zeta_{p^2}^q v^q b_1^q \\ &= (\zeta_p - 1)^r \sum_{q=0}^{s} \binom{s}{q} (-1)^{s-q}\end{aligned}$$

since $\zeta_{p^2} v b_1 = 1$. Thus, for $s \geq 1$, (8.4) holds since the sum above is 0. For $s = 0$, one has

$$\langle g a_v - 1, (\gamma^p - 1)^r (\gamma u - 1)^s\rangle = (\zeta_p - 1)^r,$$

in which case (8.4) holds since $r \cdot \operatorname{ord}(\zeta_p - 1) = re' \geq j + rj'$. It follows that $\dfrac{g a_v - 1}{\pi^j} \in H$.

An application of Proposition 7.1.3 then shows that H is of the form claimed. □

Proposition 8.4.1. *Let H be an R-Hopf order in KC_{p^2} that induces the short exact sequence $R \to H(i) \to H \to H(j) \to R$. Suppose H^* can be written in the form*

$$H^* = R\left[\frac{\gamma^p - 1}{\pi^{j'}}, \frac{\gamma u - 1}{\pi^{i'}}\right],$$

where $u = \sum_{m=0}^{p-1} b_m \eta_m \in K\langle \gamma^p \rangle$. *Then either* $i \geq pj$ *or* $j' \geq pi'$.

Proof. By Lemma 8.4.1, H has the form

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

for some unit v in R. Now, by [Ch00, 31.3],

$$\text{ord}(\zeta_p v^p - 1) \geq pj + i' \text{ and } \text{ord}(v^p - 1) \geq j + pi',$$

and so, by [Ch00, 31.4], either $i \geq pj$ or $j' \geq pi'$. □

So it remains to show that H^* can be written in the form of Lemma 8.4.1. We begin with the case $p = 2$. Let H be an R-Hopf order in KC_4, $\langle g \rangle = C_4$. Then $H = R[\frac{g^2-1}{\pi^i}, \Psi]$, where Ψ is an element of KC_4 for which $s(\Psi)$ is the generator $\frac{\overline{g}-1}{\pi^j}$ of the Larson order $H(j)$. Since $KC_4 = Ke_0 \otimes Ke_1 \otimes Ke_2 \otimes Ke_3$, Ψ has the form

$$\Psi = a_0 e_0 + a_1 e_1 + a_2 e_2 + a_3 e_3$$

for some elements $a_0, a_1, a_2, a_3 \in K$. Let e_0', e_1' be the idempotents in $K\langle \overline{g} \rangle$. Since $s(\Psi) = a_0 e_0' + a_2 e_2'$, $a_0 = 0$ and $a_2 = c = \frac{\zeta_4^2 - 1}{\pi^j}$. Thus $\Psi = a_1 e_1 + c e_2 + a_3 e_3$.

Put $h = \frac{g^2-1}{\pi^i}$. Then an R-basis for H is

$$\{1, h, \Psi, h\Psi\}.$$

Now, let ι_m be the idempotents in $K\hat{C}_4$, and let

$$\Phi = b_0 \iota_0 + b_1 \iota_1 + b_2 \iota_2 + b_3 \iota_3$$

be an element in $K\hat{C}_4$. Let $b_0 = 0$ and $b_2 = d = \frac{\zeta_4^2 - 1}{\pi^{i'}}$. We seek conditions on Φ such that

$$\langle H, \Phi \rangle \subseteq R.$$

But these can be found by choosing b_1 and b_3 such that

$$\langle \Psi, \Phi \rangle = 0,$$
$$\langle (g^2 - 1)\Psi, \Phi \rangle = 0.$$

The system above corresponds to a system of equations

$$\langle a_1e_1 + ce_2 + a_3e_3, b_1\iota_1 + d\iota_2 + b_3\iota_3\rangle = 0,$$
$$\langle a_1e_1 + a_3e_3, b_1\iota_1 + d\iota_2 + b_3\iota_3\rangle = 0,$$

which yields the 2×2 linear system

$$\begin{pmatrix} a_1\zeta_4^{-1} + c\zeta_4^{-2} + a_3\zeta_4^{-3} & a_1\zeta_4^{-3} + c\zeta_4^{-2} + a_3\zeta_4^{-1} \\ a_1\zeta_4^{-1} + a_3\zeta_4^{-3} & a_1\zeta_4^{-3} + a_3\zeta_4^{-1} \end{pmatrix}\begin{pmatrix} b_1 \\ b_3 \end{pmatrix} = \begin{pmatrix} (a_1 - c + a_3)d \\ (a_1 + a_3)d \end{pmatrix},$$

whose solution is readily obtained as

$$b_1 = \frac{\zeta_4 x - 1}{\pi^{i'}}, \quad b_3 = \frac{\zeta_4^3 x - 1}{\pi^{i'}}, \quad \text{with } x = \frac{a_3 + a_1}{a_3 - a_1}.$$

Thus

$$\Phi = \frac{\zeta_4 x - 1}{\pi^{i'}}\iota_1 + \frac{\zeta_4^2 - 1}{\pi^{i'}}\iota_2 + \frac{\zeta_4^3 x - 1}{\pi^{i'}}\iota_3 = \frac{\gamma a_x - 1}{\pi^{i'}}.$$

Now, let $A = R[\frac{\gamma^2-1}{\pi^{j'}}]$ and let $J = A[\frac{\gamma a_x - 1}{\pi^{i'}}]$. Since $\langle H, \Phi\rangle \subseteq R$, $\langle H, J\rangle \subseteq R$. An application of Proposition 7.1.3 then shows that

$$H^* = R\left[\frac{\gamma^2 - 1}{\pi^{j'}}, \frac{\gamma a_x - 1}{\pi^{i'}}\right].$$

Hence H^* is in the form of Lemma 8.4.1.

We repeat this calculation for $p = 3$. Put $\zeta = \zeta_9$. Let H be an R-Hopf order in KC_9, $C_9 = \langle g\rangle$. Then $H = R[\frac{g^3-1}{\pi^i}, \Psi]$, where Ψ is an element of KC_9 for which $s(\Psi) = \frac{\overline{g}-1}{\pi^j}$ generates the Larson order $H(j)$. We can assume that Ψ has the form

$$\Psi = c_0e_0 + a_1e_1 + a_2e_2 + c_1e_3 + a_4e_4 + a_5e_5 + c_2e_6 + a_7e_7 + a_8e_8$$

for some elements $a_1, a_2, a_4, a_5, a_7, a_8 \in K$, and $c_0 = 0$, $c_1 = \frac{\zeta^3-1}{\pi^j}$, $c_2 = \frac{\zeta^6-1}{\pi^j}$. Put $h = \frac{g^3-1}{\pi^i}$. An R-basis for H is

$$\left\{1, h, h^2, \Psi, h\Psi, h^2\Psi, \Psi^2, h\Psi^2, h^2\Psi^2\right\}.$$

Now, let ι_m denote the idempotents in $K\hat{C}_9$, and let

$$\Phi = d_0\iota_0 + b_1\iota_1 + b_2\iota_2 + d_1\iota_3 + b_4\iota_4 + b_5\iota_5 + d_2\iota_6 + b_7\iota_7 + b_8\iota_8$$

be an element of $K\hat{C}_9$ with $d_0 = 0$, $d_1 = \frac{\zeta^3-1}{\pi^{i'}}$, and $d_2 = \frac{\zeta^6-1}{\pi^{i'}}$. We seek conditions on Φ such that $\langle H, \Phi\rangle \subseteq R$. But these can be found by choosing $b_1, b_2, b_4, b_5, b_7, b_8$ such that

$$\begin{aligned}
\langle \Psi, \Phi\rangle &= 0,\\
\langle (g^3-1)\Psi, \Phi\rangle &= 0,\\
\langle (g^3-1)^2\Psi, \Phi\rangle &= 0,\\
\langle \Psi^2, \Phi\rangle &= 0,\\
\langle (g^3-1)\Psi^2, \Phi\rangle &= 0,\\
\langle (g^3-1)^2\Psi^2, \Phi\rangle &= 0.
\end{aligned}$$

This system corresponds to the system of equations

$$\begin{aligned}
&\langle a_1e_1 + a_2e_2 + c_1e_3 + a_4e_4 + a_5e_5 + c_2e_6 + a_7e_7 + a_8e_8,\\
&\quad b_1\iota_1 + b_2\iota_2 + d_1\iota_3 + b_4\iota_4 + b_5\iota_5 + d_2\iota_6 + b_7\iota_7 + b_8\iota_8\rangle = 0;\\
&\langle (\zeta-1)a_1e_1 + (\zeta^2-1)a_2e_2 + (\zeta-1)a_4e_4 + (\zeta^2-1)a_5e_5\\
&\quad +(\zeta-1)a_7e_7 + (\zeta^2-1)a_8e_8,\\
&\qquad b_1\iota_1 + b_2\iota_2 + d_1\iota_3 + b_4\iota_4 + b_5\iota_5 + d_2\iota_6 + b_7\iota_7 + b_8\iota_8\rangle = 0;\\
&\langle (\zeta-1)^2a_1e_1 + (\zeta^2-1)^2a_2e_2 + (\zeta-1)^2a_4e_4 + (\zeta^2-1)^2a_5e_5\\
&\quad +(\zeta-1)^2a_7e_7 + (\zeta^2-1)^2a_8e_8,\\
&\qquad b_1\iota_1 + b_2\iota_2 + d_1\iota_3 + b_4\iota_4 + b_5\iota_5 + d_2\iota_6 + b_7\iota_7 + b_8\iota_8\rangle = 0;\\
&\langle a_1^2e_1 + a_2^2e_2 + c_1^2e_3 + a_4^2e_4 + a_5^2e_5 + c_2^2e_6 + a_7^2e_7 + a_8^2e_8,\\
&\quad b_1\iota_1 + b_2\iota_2 + d_1\iota_3 + b_4\iota_4 + b_5\iota_5 + d_2\iota_6 + b_7\iota_7 + b_8\iota_8\rangle = 0;\\
&\langle (\zeta-1)a_1^2e_1 + (\zeta^2-1)a_2^2e_2 + (\zeta-1)a_4^2e_4 + (\zeta^2-1)a_5^2e_5\\
&\quad +(\zeta-1)a_7^2e_7 + (\zeta^2-1)a_8^2e_8,\\
&\qquad b_1\iota_1 + b_2\iota_2 + d_1\iota_3 + b_4\iota_4 + b_5\iota_5 + d_2\iota_6 + b_7\iota_7 + b_8\iota_8\rangle = 0;\\
&\langle (\zeta-1)^2a_1^2e_1 + (\zeta^2-1)^2a_2^2e_2 + (\zeta-1)^2a_4^2e_4 + (\zeta^2-1)^2a_5^2e_5\\
&\quad +(\zeta-1)^2a_7^2e_7 + (\zeta^2-1)^2a_8^2e_8,\\
&\qquad b_1\iota_1 + b_2\iota_2 + d_1\iota_3 + b_4\iota_4 + b_5\iota_5 + d_2\iota_6 + b_7\iota_7 + b_8\iota_8\rangle = 0.
\end{aligned}$$

Set

$$\begin{aligned}
A &= a_1\zeta^{-1} + a_4\zeta^{-4} + a_7\zeta^{-7}, & B &= a_1\zeta^{-2} + a_4\zeta^{-8} + a_7\zeta^{-5},\\
C &= a_1 + a_4 + a_7, & E &= a_2\zeta^{-2} + a_5\zeta^{-5} + a_8\zeta^{-8},\\
F &= a_2\zeta^{-4} + a_5\zeta^{-1} + a_8\zeta^{-7}, & G &= a_2 + a_5 + a_8,\\
A' &= a_1^2\zeta^{-1} + a_4^2\zeta^{-4} + a_7^2\zeta^{-7}, & B' &= a_1^2\zeta^{-2} + a_4^2\zeta^{-8} + a_7^2\zeta^{-5},\\
C' &= a_1^2 + a_4^2 + a_7^2, & E' &= a_2^2\zeta^{-2} + a_5^2\zeta^{-5} + a_8^2\zeta^{-8},\\
F' &= a_2^2\zeta^{-4} + a_5^2\zeta^{-1} + a_8^2\zeta^{-7}, & G' &= a_2^2 + a_5^2 + a_8^2,\\
J &= c_1\zeta^{-3} + c_2\zeta^{-6}, & K &= c_1\zeta^{-6} + c_2\zeta^{-3},\\
J' &= c_1^2\zeta^{-3} + c_2^2\zeta^{-6}, & K' &= c_1^2\zeta^{-6} + c_2^2\zeta^{-3}.
\end{aligned}$$

Note that

$$\begin{aligned}
K &= c_1\zeta^{-6} + c_2\zeta^{-3}\\
&= \zeta^{-2}\left(\frac{\zeta-1}{\pi^j}\right) + \zeta^{-1}\left(\frac{\zeta^2-1}{\pi^j}\right)\\
&= 0.
\end{aligned}$$

Using the relation $\langle e_m, \iota_n\rangle = \zeta^{-mn}/9$, one obtains the 6×6 linear system

$$M\begin{pmatrix} b_1\\ b_2\\ b_4\\ b_5\\ b_7\\ b_8\end{pmatrix} = \begin{pmatrix}
(-\zeta^{-3}C - \zeta^{-6}G - c_1 - c_2)d_1 + (-\zeta^{-6}C - \zeta^{-3}G - c_1 - c_2)d_2\\
(-\zeta^{-3}d_1 - \zeta^{-6}d_2)C\\
(-\zeta^{-6}d_1 - \zeta^{-3}d_2)G\\
(-\zeta^{-3}C' - \zeta^{-6}G' - c_1 - c_2)d_1 + (-\zeta^{-6}C' - \zeta^{-3}G' - c_1 - c_2)d_2\\
(-\zeta^{-3}d_1 - \zeta^{-6}d_2)C'\\
(-\zeta^{-6}d_1 - \zeta^{-3}d_2)G'
\end{pmatrix},$$

where M is the matrix

$$\begin{pmatrix}
A+E+J & B+F & \zeta^{-3}A + \zeta^{-6}E + J & \zeta^{-3}B + \zeta^{-6}F\\
A & B & \zeta^{-3}A & \zeta^{-3}B\\
E & F & \zeta^{-6}E & \zeta^{-6}F\\
A'+E'+J' & B'+F'+K' & \zeta^{-3}A' + \zeta^{-6}E' + J' & \zeta^{-3}B' + \zeta^{-6}F' + K'\\
A' & B' & \zeta^{-3}A' & \zeta^{-3}B'\\
E' & F' & \zeta^{-6}E' & \zeta^{-6}F'
\end{pmatrix}$$

$$
\left.\begin{matrix}
\zeta^{-6}A+\zeta^{-3}E+J & \zeta^{-6}B+\zeta^{-3}E \\
\zeta^{-6}A & \zeta^{-6}B \\
\zeta^{-3}E & \zeta^{-3}F \\
\zeta^{-6}A'+\zeta^{-3}E'+J' & \zeta^{-6}B'+\zeta^{-3}E'+K' \\
\zeta^{-6}A' & \zeta^{-6}B' \\
\zeta^{-3}E' & \zeta^{-3}F'
\end{matrix}\right)
$$

This system is equivalent to the system

$$
\left(\begin{array}{cccccc|c}
1 & 0 & 1 & 0 & 1 & 0 & \frac{-3}{\pi^{i'}} \\
\frac{A}{B} & 1 & \zeta^{-3}\frac{A}{B} & \zeta^{-3} & \zeta^{-6}\frac{A}{B} & \zeta^{-6} & \frac{-3}{\pi^{i'}}\frac{C}{B} \\
1 & \frac{F}{E} & \zeta^{-6} & \zeta^{-6}\frac{F}{E} & \zeta^{-3} & \zeta^{-3}\frac{F}{E} & 0 \\
J' & K' & J' & K' & J' & K' & \frac{3(c_1^2+c_2^2)}{\pi^{i'}} \\
\frac{A'}{B'} & 1 & \zeta^{-3}\frac{A'}{B'} & \zeta^{-3} & \zeta^{-6}\frac{A'}{B'} & \zeta^{-6} & \frac{-3}{\pi^{i'}}\frac{C'}{B'} \\
1 & \frac{F'}{E'} & \zeta^{-6} & \zeta^{-6}\frac{F'}{E'} & \zeta^{-3} & \zeta^{-3}\frac{F'}{E'} & 0
\end{array}\right),
$$

which reduces to the system

$$
\left(\begin{matrix}
1 & 0 & 1 & 0 & 1 \\
\frac{A}{B}-\frac{A'}{B'} & 0 & \zeta^{-3}\left(\frac{A}{B}-\frac{A'}{B'}\right) & 0 & \zeta^{-6}\left(\frac{A}{B}-\frac{A'}{B'}\right) \\
0 & \frac{F}{E}-\frac{F'}{E'} & 0 & \zeta^{-6}\left(\frac{F}{E}-\frac{F'}{E'}\right) & 0 \\
0 & 1 & 0 & 1 & 0 \\
\frac{A'}{B'} & 1 & \zeta^{-3}\frac{A'}{B'} & \zeta^{-3} & \zeta^{-6}\frac{A'}{B'} \\
1 & \frac{F'}{E'} & \zeta^{-6} & \zeta^{-6}\frac{F'}{E'} & \zeta^{-3}
\end{matrix}\right.
$$

$$
\left.\begin{array}{c|c}
0 & \frac{-3}{\pi^{i'}} \\
0 & \frac{-3}{\pi^{i'}}\left(\frac{C}{B}-\frac{C'}{B'}\right) \\
\zeta^{-3}\left(\frac{F}{E}-\frac{F'}{E'}\right) & 0 \\
1 & \frac{-3}{\pi^{i'}} \\
\zeta^{-6} & \frac{-3}{\pi^{i'}}\frac{C'}{B'} \\
\zeta^{-3}\frac{F'}{E'} & 0
\end{array}\right),
$$

and ultimately to the system

$$\left(\begin{array}{cccccc|c} 1 & 0 & 1 & 0 & 1 & 0 & \frac{-3}{\pi^{i'}} \\ 1 & 0 & \zeta^{-3} & 0 & \zeta^{-6} & 0 & \frac{3}{\pi^{i'}}\left(\frac{BC'-CB'}{AB'-BA'}\right) \\ 0 & 1 & 0 & \zeta^{-6} & 0 & \zeta^{-3} & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & \frac{-3}{\pi^{i'}} \\ 0 & 1 & 0 & \zeta^{-3} & 0 & \zeta^{-6} & \frac{3}{\pi^{i'}}\left(\frac{CA'-AC'}{AB'-BA'}\right) \\ 1 & 0 & \zeta^{-6} & 0 & \zeta^{-3} & 0 & 0 \end{array}\right).$$

Now, the required values of $b_1, b_2, b_4, b_5, b_7, b_8$ satisfy

$$\begin{aligned} b_1 + b_4 + b_7 &= \frac{-3}{\pi^{i'}}, \\ b_1 + \zeta^{-3}b_4 + \zeta^{-6}b_7 &= \frac{3}{\pi^{i'}}\left(\frac{BC'-CB'}{AB'-BA'}\right), \\ b_2 + \zeta^{-6}b_5 + \zeta^{-3}b_8 &= 0, \\ b_2 + b_5 + b_8 &= \frac{-3}{\pi^{i'}}, \\ b_2 + \zeta^{-3}b_5 + \zeta^{-6}b_8 &= \frac{3}{\pi^{i'}}\left(\frac{CA'-AC'}{AB'-BA'}\right), \\ b_1 + \zeta^{-6}b_4 + \zeta^{-3}b_7 &= 0. \end{aligned} \tag{8.15}$$

Let x and y be elements of K, and set $b_1 = \frac{\zeta x-1}{\pi^{i'}}$, $b_2 = \frac{\zeta^2 y-1}{\pi^{i'}}$, $b_4 = \frac{\zeta^4 x-1}{\pi^{i'}}$, $b_5 = \frac{\zeta^5 y-1}{\pi^{i'}}$, $b_7 = \frac{\zeta^7 x-1}{\pi^{i'}}$, and $b_8 = \frac{\zeta^8 y-1}{\pi^{i'}}$. Then, with

$$\begin{aligned} x &= \zeta^{-1}\left(\frac{BC'-CB'}{AB'-BA'}\right), \\ y &= \zeta^{-2}\left(\frac{CA'-C'A}{AB'-BA'}\right), \end{aligned}$$

the equations in (8.15) are satisfied.

Now

$$\begin{aligned} \Phi = \frac{\zeta x-1}{\pi^{i'}}\iota_1 + \frac{\zeta^2 y-1}{\pi^{i'}}\iota_2 + \frac{\zeta^3-1}{\pi^{i'}}\iota_3 + b_4\frac{\zeta^4 x-1}{\pi^{i'}}\iota_4 \\ + \frac{\zeta^5 y-1}{\pi^{i'}}\iota_5 + \frac{\zeta^6-1}{\pi^{i'}}\iota_6 + \frac{\zeta^7 x-1}{\pi^{i'}}\iota_7 + \frac{\zeta^8 y-1}{\pi^{i'}}\iota_8 = \frac{\gamma u-1}{\pi^{i'}}, \end{aligned}$$

where $u = \eta_0 + x\eta_1 + y\eta_2 \in K\langle\gamma^3\rangle$, with η_m the idempotents in $K\langle\gamma^3\rangle$. With this definition of Φ, we have

$$\langle H, \Phi\rangle \subseteq R.$$

Let $A = R[\frac{\gamma^3-1}{\pi^{j'}}]$, and let $J = A[\frac{\gamma u-1}{\pi^{i'}}]$. Since $\langle H, \Phi\rangle \subseteq R$, $\langle H, J\rangle \subseteq R$. An application of Proposition 7.1.3 then yields

$$H^* = R\left[\frac{\gamma^3-1}{\pi^{j'}}, \frac{\gamma u-1}{\pi^{i'}}\right].$$

8.5 Chapter Exercises

Exercises for §8.1

1. Let K be a finite extension of $\mathbb{Q}_2$ with $\mathrm{ord}(2) = e$. Let H be an R-Hopf order in KC_4. Prove that there is no short exact sequence of R-Hopf orders of the form
$$R \to H(e/2) \to H \to H(e/2) \to R.$$
2. Suppose $\zeta_{p^2} \in K$, let H be an R-Hopf order in KC_{p^2}, and let
$$R \to H(i) \to H \to H(j) \to R$$
be a short exact sequence with $pj > i$. Prove that $\mathrm{ord}(1 - \zeta_{p^2}) \geq i' + (j/p)$.

Exercises for §8.2

3. Let $h : C_m \to G$ be a function with $h(1) = 1$. Let $f_h : C_m \times C_m \to G$ be defined as
$$f_h(\tau^i, \tau^j) = h(\tau^i)(h(\tau^{i+j}))^{-1}h(\tau^j)$$
for $i, j = 0, \ldots, m-1$. Prove that f_h is a cocycle.
4. Prove Proposition 8.2.1.
5. Compute all of the non-equivalent extensions in $E(\mathbb{Z}, C_3)$.
6. Compute all of the non-equivalent extensions in $E(\mathbb{Z}/(p^2), C_p)$.

Exercises for §8.3

7. Prove Proposition 8.3.8.
8. Prove Lemma 8.3.1.
9. Prove that the R-Hopf orders $A(i, j, v)$ and $A(i, j, w)$ are equal if and only if $\mathrm{ord}(v - w) \geq i' + j$.
10. Let $A(i, j, v)$ be a Greither order in KC_{p^2}.
    (a) Show that $A(i, j, v^{-1})$ is a Greither order in KC_{p^2}.
    (b) Show that $A(i, j, v) = A(i, j, v^{-1})$ if and only if $p = 2$.

11. Let $H(i, j)$ be a Larson order in KC_{p^2}. Find conditions on i, j so that the linear dual $H(i, j)^*$ is a Larson order in KC_{p^2}.
12. Let $A(i, j, u)$ be an R-Hopf order in KC_{p^2}. Show that $\text{ord}(1-u) \geq i' + (j/p)$.
13. Suppose $A(i, j, v)$ is a Greither order with $\text{ord}(1 - \zeta_{p^2} v) \geq i'$. Show that there exists an R-Hopf order of the form $H(a, b)^*$ for which $H(a, b)^* \subseteq A(i, j, v)$.
14. By Proposition 8.3.5, $C/B \cong U_{pi'+j}(R)/U^p_{i'+j}(R)$, and by Proposition 8.2.3, $E(U_j(R), C_p) \cong U_j(R)/U^p_j(R)$. Is C/B a subgroup of $E(U_j(R), C_p)$?

Exercises for §8.4

15. How would one generalize the results of §8.4 to $p > 3$?