New York Journal of Mathematics

New York J. Math. **23** (2017) 11–39.

Finite group scheme extensions, and Hopf orders in KC_p^2 over a characteristic p discrete valuation ring

G. Griffith Elder and **Robert G. Underwood**

Abstract. Let p be prime. Let R be a discrete valuation ring of characteristic p with field of fractions K. Let C_p^2 denote the elementary abelian group of order p^2. In this paper we use Greither's approach for classifying short exact sequences of finite R-group schemes to classify R-Hopf orders $\mathcal{H}$ in the group ring KC_p^2, reproducing a result of Tossici. We then go further by providing an explicit description of the correspondence between these Hopf orders $\mathcal{H}$ and their duals $\mathcal{H}^*$, and also by explicitly describing their endomorphisms rings. Thus we are able to identify the Raynaud orders within this classification.

Contents

1. Introduction

Let p be prime, let R be a discrete valuation ring of characteristic p with quotient field K, and let C_p^2 be the elementary abelian group of order p^2. The group ring KC_p^2 is a Hopf algebra over K with the usual comultiplication,

Received May 2, 2016.

2010 *Mathematics Subject Classification.* 16T05, 14L15, 20J05.

Key words and phrases. Hopf orders, group schemes, extensions, cohomology groups.

ISSN 1076-9803/2017

counit and antipode. Hopf orders $\mathcal{H}$ in KC_p^2 are Hopf algebras $\mathcal{H}$ that are finitely generated and free (and thus flat) over R such that $K\otimes_R\mathcal{H}\cong KC_p^2$ as Hopf algebras over K. Let $\mu_{p,K}^2$ denote the spectrum of KC_p^2. Hopf orders $\mathcal{H}$ correspond to models $\mathcal{G}$ of $\mu_{p,K}^2$, via the functor $\mathrm{Hom}_{R\text{-alg}}(\mathcal{H},-)=\mathcal{G}$. Namely, each model $\mathcal{G}$ is a finite group scheme over R whose generic fiber $\mathcal{G}_K$ is isomorphic to $\mu_{p,K}^2$ (i.e., group schemes where the Cartier dual of its generic fiber is the constant group scheme C_p^2). In this paper, we are interested in classifying these Hopf orders in KC_p^2, or equivalently, these models of $\mu_{p,K}^2$.

Tate and Oort settled this classification when the group C_p is cyclic of order p for both characteristics of the field, $\mathrm{char}(K)=p$ or 0 [TO70]. Greither settled this classification for a large class when the group C_{p^2} is cyclic of order p^2, $\mathrm{char}(K)=0$ and K contains a primitive pth root of unity ξ_p [Gre92]. Byott's classification of cleft extensions settled the classification when the group has order p^2, assuming $\mathrm{char}(K)=0$ and $\xi_p\in K$ for C_p^2, or $\xi_{p^2}\in K$ for C_{p^2} [By93, §8]. See [By93, page 278 *Added in proof*]. Assuming $\xi_{p^2}\in K$, [Und94] observed that the Hopf orders in KC_{p^2} that lie outside of Greither's large class have their duals back within the class. More recently, using the methods of Sekiguchi and Suwa, Tossici classified all Hopf orders when the group has order p^2 in either characteristic [Tos10]. In this paper, we reproduce Tossici's result for the group C_p^2 in $\mathrm{char}(K)=p$, using the approach in [Gre92]. It may therefore, in part, be viewed as an exposition of Greither's approach, although, of course, the change in characteristic and group result in some significant (indeed, important simplifying) differences.

We begin in §2 by reproducing the Tate–Oort classification of Hopf orders in KC_p. In §3, we describe the Hopf orders in KC_p^2 and their duals. In §4, we classify the Hopf orders in KC_p^2 based upon a classification of group scheme extensions that follows [Gre92].

The description of the Hopf orders in KC_p^2 in Proposition 3.4 is (after a simple notational change) exactly the description of [Tos10]. Still, this description arose elsewhere, growing as it did out of a recent development in Galois module theory. So recall that one motivation for classifying Hopf orders is that Hopf orders "tame" wild ramification for Galois module theory [Chi00]. Under certain hypotheses, Bondarko makes this connection between "freeness over the associated order" (the main object of Galois module theory) and Hopf orders work in both directions [Bon00]. Thus Galois scaffolds, which provide an alternate approach to Galois module theory under wild ramification, can be used to generate Hopf orders [ByE14, §5], and it is these Hopf orders that motivate the description in Proposition 3.4.

The explicit description of Hopf orders in KC_p^2 is linked with explicit descriptions for their duals in Proposition 3.2. Using Dieudonné theory, Koch has separately classified these Hopf orders, Hopf orders in the dual Hopf algebra $(KC_p^2)^*$, as they are primitively generated [Koc16]. This means that given the correspondence between Hopf orders in KC_p^2 and in $(KC_p^2)^*$ provided here by Theorem 3.6, the classification result Theorem 4.6 possesses three different proofs, due to Tossici, Koch and here based upon the approach of Greither.

All the details that are available in our explicit descriptions (Propositions 3.4, 3.2, and Theorem 4.6) can then be put to use, as we do in §5, to describe the parameter space for these Hopf orders, as well as their endomorphism rings. Here we are able to go further than the results in [Tos10, Koc16]. In doing so, we are able to identify where the Raynaud orders appear in our classification.

In §6, we conclude with a simple consequence of our results.

Acknowledgements. We thank Professor Cornelius Greither for his advice concerning the argument in [Gre92]. We thank the referee for suggesting that we address $\mu = 0$ (Proposition 5.2), and for several clarifying remarks. The first author thanks the University of Exeter for its hospitality during 2014/2015 when some of the details of §4 were worked out.

2. Hopf orders in KC_p

Let R be a discrete valuation ring with field of fractions K and $\operatorname{char}(R) = p$. Let σ generate C_p, let $i \geq 0$ be an integer and let

$$\mathcal{H}_i = R\left[\frac{\sigma - 1}{\pi^i}\right].$$

Since $(\sigma - 1)^p = 0$ in KC_p, it is easy to see that $\mathcal{H}_i$ is both closed under multiplication and a free R-module of rank p. Since $RC_p \subseteq \mathcal{H}_i$, we clearly have $K\mathcal{H}_i = KC_p$. Comultiplication on σ is grouplike, therefore, letting $x = (\sigma - 1)/\pi^i$ we have

$$\Delta(x) = x \otimes 1 + 1 \otimes x + \pi^i x \otimes x \in \mathcal{H}_i \otimes \mathcal{H}_i.$$

As a result, $\mathcal{H}_i$ is a Hopf order in KC_p.

Let KC_p^* be the linear dual of KC_p, and let $\{e_i\}_{i\in\mathbb{F}_p}$ be the K-basis for KC_p^* which is dual to the basis $\{\sigma^j\}_{j\in\mathbb{F}_p}$ for KC_p. We have $\langle e_i, \sigma^j\rangle = \delta_{i,j}$, the Kronecker delta function. It is well-known that KC_p^* is a K-Hopf algebra. Multiplication in KC_p^* is determined by $e_ie_j = \delta_{i,j}$. Thus $\{e_i\}_{i\in\mathbb{F}_p}$ is an orthonormal basis, and $e_0 + e_1 + \cdots + e_{p-1}$ is the multiplicative identity. The counit is determined by $\varepsilon(e_i) = \delta_{i,0}$, comultiplication is determined by $\Delta(e_i) = \sum_{j\in\mathbb{F}_p} e_j \otimes e_{i-j}$, and the antipode satisfies $S(e_i) = e_{-i}$.

Lemma 2.1. *Let $\xi_1 = \sum_{r=1}^{p-1} re_r \in KC_p^*$. Then $\langle \xi_1, (\sigma-1)^j\rangle = \delta_{1,j}$, and $RC_p^* = R[\xi_1]$ is an R-Hopf algebra with $\xi_1^p = \xi_1$. The counit map satisfies $\varepsilon(\xi_1) = 0$, comultiplication is given as $\Delta(\xi_1) = \xi_1 \otimes 1 + 1 \otimes \xi_1$, namely ξ_1 is primitive, and the antipode satisfies $S(\xi_1) = -\xi_1$.*

Proof. From the expansion

$$x^j = ((x+1)-1)^j = \sum_{r=0}^{j} \binom{j}{r} (-1)^{j-r} \sum_{i=0}^{r} \binom{r}{i} x^i$$
$$= \sum_{i=0}^{j} \sum_{r=i}^{j} \binom{j}{r} \binom{r}{i} (-1)^{j-r} x^i$$

we obtain the identity $\delta_{i,j} = \sum_{r=i}^{j} \binom{j}{r}\binom{r}{i}(-1)^{j-r}$. Using this identity, we see that the elements

$$\xi_i = \sum_{r=i}^{p-1} \binom{r}{i} e_r$$

satisfy $\langle \xi_i, (\sigma-1)^j \rangle = \delta_{i,j}$. Since $\{(\sigma-1)^j\}_{j=0}^{p-1}$ is an R-basis for RC_p, $\{\xi_i\}_{i=0}^{p-1}$ is an R-basis for RC_p^*. The identity element is $\xi_0 = e_0 + \cdots + e_{p-1}$, which we denote as $1 \in RC_p^*$. For $1 \leq i \leq p-1$,

$$\xi_1\xi_i - i\xi_i = \sum_{r=i+1}^{p-1} (r-i) \binom{r}{i} e_r = (i+1)\xi_{i+1},$$

therefore, $(\xi_1 - i)\xi_i = (i+1)\xi_{i+1}$. From this we see that $(\xi_1 - p + 1)\xi_{p-1} = 0$ and using induction that

$$\binom{\xi_1}{i} = \xi_i$$

for $0 \leq i \leq p-1$. Recall the binomial coefficient

$$\binom{x}{i} = x(x-1)\ldots(x-i+1)/i! \in \mathbb{Q}[x].$$

This means that the matrix M that maps $\xi_1, \xi_1^2, \ldots, \xi_1^{p-1}$ to $\xi_1, \xi_2, \ldots, \xi_{p-1}$ is $\mathbb{F}_p$-valued, upper triangular with the reciprocals of $1!, 2!, \ldots, (p-1)!$ down the diagonal. As a result, M is invertible over R, and $RC_p^* = R[\xi_1]$. Of course, $\xi_1^p = \xi_1$ follows directly from the expression for ξ_1 and the fact that $\{e_r\}_{r\in\mathbb{F}_p}$ is an orthonormal basis. Since $\varepsilon(e_r) = \delta_{r,0}$, $\varepsilon(\xi_1) = 0$, and since $S(e_r) = e_{-r}$, $S(\xi_1) = \sum_{r=1}^{p-1}(p-r)e_r = -\xi_1$. Finally, for $0 \leq i, a+b < p$, we have

$$\langle \xi_i, (\sigma-1)^{a+b} \rangle = \delta_{i,a+b} = \sum_{r=0}^{i} \delta_{r,a}\delta_{i-r,b}$$
$$= \mathrm{mult}(\langle \Delta(\xi_i), (\sigma-1)^a \otimes (\sigma-1)^b \rangle),$$

and so,

$$\Delta(\xi_i) = \sum_{r=0}^{i} \xi_r \otimes \xi_{i-r}. \tag{1}$$

In particular, ξ_1 is primitive. Of course, this statement also follows directly from the description of ξ_1 and comultiplication on the e_r. Observe that

$$\begin{aligned}\Delta(\xi_1) = \sum_{r=0}^{p-1} r\Delta(e_r) &= \sum_{r=0}^{p-1} r \sum_{i=0}^{p-1} e_i \otimes e_{r-i} \\ &= \sum_{k,l=0}^{p-1} (k+l) e_k \otimes e_l = \xi_1 \otimes 1 + 1 \otimes \xi_1. \qquad \square\end{aligned}$$

Direct computation, using the orthonormal basis $\{e_r\}_{r\in\mathbb{F}_p}$ for RC_p^*, yields $\operatorname{disc}(RC_p^*) = R$.

Proposition 2.2. *Let $i \geq 0$ be an integer and $\beta = \pi^i\xi_1$. Then $R[\beta]$ is an R-Hopf algebra contained in RC_p^* with $\beta^p = \pi^{(p-1)i}\beta$; its coalgebra structure is defined by counit $\varepsilon(\beta) = 0$, comultiplication $\Delta(\beta) = \beta \otimes 1 + 1 \otimes \beta$, and antipode $S(\beta) = -\beta$. We also have $R[\beta] = \mathcal{H}_i^*$ with discriminant* $\operatorname{disc}(R[\beta]) = (\pi^{p(p-1)i})$.

Proof. The properties of $R[\beta]$ as an R-Hopf algebra follow immediately from Lemma 2.1. It remains to prove the last two statements. Since $\{(\sigma-1)^r\pi^{-ri}\}_{r=0}^{p-1}$ is an R-basis for $\mathcal{H}_i$, an R-basis for $\mathcal{H}_{i_2}^*$ is given by $\{\pi^{ri}\binom{\xi_1}{r}\}_{r=0}^{p-1}$. The matrix that maps $\{\pi^{ri}\xi_1^r\}_{r=0}^{p-1}$ to $\{\pi^{ri}\binom{\xi_1}{r}\}_{r=0}^{p-1}$ is R-valued, upper triangular with determinant a unit in R. Thus $\mathcal{H}_i^* = R[\pi^i\xi_1]$. To determine $\operatorname{disc}(R[\pi^i\xi_1])$, we observe that the matrix that maps $\{\xi_1^r\}_{r=0}^{p-1}$ to $\{\pi^{ri}\xi_1^r\}_{r=0}^{p-1}$ is diagonal with determinant $\pi^{p(p-1)i/2}$. Hence the module index $[R[\xi_1] : R[\pi^i\xi_1]] = (\pi^{p(p-1)i/2})$. As a result, since $\operatorname{disc}(R[\xi_1]) = R$, $\operatorname{disc}(R[\pi^i\xi_1]) = [R[\xi_1] : R[\pi^i\xi_1]]^2\operatorname{disc}(R[\xi_1]) = (\pi^{p(p-1)i})$. □

Theorem 2.3 (Tate–Oort)**.** *Hopf orders in KC_p can be expressed as $\mathcal{H}_i$ for some $i \geq 0$.*

Proof. Let $\mathcal{H}$ be an R-Hopf order in KC_p. Then $\mathcal{H}^*$ is an R-Hopf order in KC_p^* and both $\mathcal{H}$ and $\mathcal{H}^*$ are cocommutative, commutative R-Hopf algebras [Chi00, page 9, Example (1.4)]. Thus $\mathbb{D}^* = \mathrm{Hom}_{\text{R-alg}}(\mathcal{H}^*, -)$ is a finite group scheme of order p, which over K, is represented by $KC_p^* = K[\xi_1]$. By [TO70, Remark 3, p. 15], Tate and Oort's classification theorem ([TO70, Theorem 2, p. 12]) holds in characteristic p. Using [TO70, Remark 5, p. 15] for the local ring R, there is a factorization $0 = p = a \cdot 0$ for some $a \in R$ such that $\mathcal{H}^* = R[x]$ with $x^p = ax$ and $\Delta(x) = x \otimes 1 + 1 \otimes x$. This also applies to the local ring K. So, since $\xi_1^p = \xi_1$, the K-Hopf algebra $KC_p^* = K[\xi_1]$ corresponds to the factorization $0 = p = 1 \cdot 0$. Since $K\mathcal{H}^* = KC_p^*$, these factorizations are equivalent, which means that there is $u \in K^\times$ so that $1 = au^{p-1}$. Hence $a = d^{p-1}$ for some $d = v\pi^i \in R$ where $v \in R^\times$ and $i \geq 0$. Since $x^p = ax$, $y = x/v$ satisfies $y^p = \pi^{(p-1)i}y$, and $\mathcal{H}^* = R[y]/(y^p - \pi^{(p-1)i}y)$. Note $\pi^i\xi_1$ satisfies $y^p = \pi^{(p-1)i}y$. Thus $\mathcal{H}^* = R[\pi^i\xi_1]$. By Proposition 2.2, $\mathcal{H} = \mathcal{H}_i$. □

3. Hopf orders in KC_p^2

In this section, we describe a family of R-Hopf orders in KC_p^2 and give their duals in $(KC_p^2)^*$. That these are all the Hopf orders is proven in §4.

Let $C_p^2 = \langle \sigma_1, \sigma_2 \rangle$. Then $\{\sigma_1^a\sigma_2^b\}_{a,b\in\mathbb{F}_p}$ is a basis for KC_p^2, with dual basis $\{e_{a,b}\}_{a,b\in\mathbb{F}_p}$ for $(KC_p^2)^*$ satisfying $\langle e_{a,b}, \sigma_1^c\sigma_2^d\rangle = \delta_{a,c}\delta_{b,d}$. The dual $(KC_p^2)^*$ is a K-Hopf algebra. Alternatively, we may express KC_p^2 as $KC_p \otimes_K KC_p$ with $\sigma_1^a\sigma_2^b$ expressed as $\sigma^a \otimes \sigma^b$, and $(KC_p^2)^*$ as $KC_p^* \otimes_K KC_p^*$ with $e_{a,b}$ as $e_a \otimes e_b$, where e_a, e_b are defined as in §2. By abuse of notation, we use the notations $\sigma_1^a\sigma_2^b$ and $e_{a,b}$ interchangeably with $\sigma^a \otimes \sigma^b$ and $e_a \otimes e_b$, whichever is most convenient. We always express $KC_p \otimes_K KC_p$ as KC_p^2, and $KC_p^* \otimes_K KC_p^*$ as $(KC_p^2)^*$. So for example, multiplication in $(KC_p^2)^*$ is given by $e_{a,b}e_{c,d} = e_a \otimes e_b \cdot e_c \otimes e_d = e_ae_c \otimes e_be_d = \delta_{a,c}\delta_{b,d}e_c \otimes e_d = \delta_{a,c}\delta_{b,d}e_{c,d}$, hence $\{e_{a,b}\}_{a,b\in\mathbb{F}\_p}$ is an orthonormal basis with $\sum_{a,b\in\mathbb{F}_p} e_{a,b} = 1 \in (KC_p^2)^*$. The counit map is determined by $\epsilon(e_{a,b}) = \delta_{a,0}\delta_{b,0}$, comultiplication is determined by $\Delta(e_{a,b}) = \sum_{i,j\in\mathbb{F}_p} e_{i,j} \otimes e_{a-i,b-j}$, and the antipode satisfies $S(e_{a,b}) = e_{-a,-b}$.

Lemma 3.1. *Let $\xi_{1,0} = \xi_1 \otimes 1$ and $\xi_{0,1} = 1 \otimes \xi_1 \in (KC_p^2)^*$ with ξ_1 as in Lemma 2.1. Then*

$$\langle \xi_{1,0}, (\sigma_1 - 1)^j(\sigma_2 - 1)^k\rangle = \delta_{1,j}\delta_{0,k} \quad \textit{and} \quad \langle \xi_{0,1}, (\sigma_1 - 1)^j(\sigma_2 - 1)^k\rangle = \delta_{0,j}\delta_{1,k},$$

and $(RC_p^2)^* = R[\xi_{1,0}, \xi_{0,1}]$ is an R-Hopf algebra with $\xi_{1,0}$ and $\xi_{0,1}$ satisfying $x^p = x$, counit $\varepsilon(x) = 0$, comultiplication $\Delta(x) = x \otimes 1 + 1 \otimes x$, and antipode $S(x) = -x$.

Proof. Letting ξ_i, ξ_j be as in the proof of Lemma 2.1, we define

$$\xi_{i,j} = \sum_{r=i}^{p-1}\sum_{s=j}^{p-1}\binom{r}{i}\binom{s}{j}e_{r,s} = \sum_{r=i}^{p-1}\binom{r}{i}e_r \otimes \sum_{s=j}^{p-1}\binom{s}{j}e_s = \xi_i \otimes \xi_j.$$

Note that $\xi_{0,0}$ is the multiplicative identity $1 \in (KC_p^2)^*$. These satisfy

$$\begin{aligned}\langle \xi_{i,j}, (\sigma_1 - 1)^a(\sigma_2 - 1)^b\rangle &= \langle \xi_i \otimes \xi_j, (\sigma - 1)^a \otimes (\sigma - 1)^b\rangle \\ &= \langle \xi_i, (\sigma - 1)^a\rangle\langle \xi_j, (\sigma - 1)^b\rangle = \delta_{i,a}\delta_{j,b}.\end{aligned}$$

Since $\{(\sigma_1 - 1)^a(\sigma_2 - 1)^b\}_{a,b=0}^{p-1}$ is an R-basis for RC_p^2, $\{\xi_{i,j}\}_{i,j=0}^{p-1}$ is an R-basis for $(RC_p^2)^*$. Since $\{\xi_{i,j}\}_{i,j=0}^{p-1} = \{\xi_i \otimes \xi_j\}_{i,j=0}^{p-1}$ and the R-spans of $\{\xi_i\}_{i=0}^{p-1}$ and $\{\xi_1^i\}_{i=0}^{p-1}$ agree, an alternative R-basis for $(RC_p^2)^*$ is given by $\{\xi_1^i \otimes \xi_1^j\}_{i,j=0}^{p-1}$. Thus $(RC_p^2)^* = R[\xi_{1,0}, \xi_{0,1}]$. The (co)algebraic properties of the generators $\xi_{1,0}$ and $\xi_{0,1}$ are immediate from Lemma 2.1. □

Denote the polynomial $x^p - x \in \mathbb{Z}[x]$, which is additive in characteristic p, by $\wp(x) = x^p - x$. Let ν_K denote the valuation normalized so that $\nu_K(K^\times) = \mathbb{Z}$.

Proposition 3.2. *Given integers $i_1, i_2 \geq 0$ and $\mu \in K$, let*

$$\beta_1 = \pi^{i_1}(\xi_{1,0} - \mu\xi_{0,1}) \quad \text{and} \quad \beta_2 = \pi^{i_2}\xi_{0,1} \in (RC_p^2)^*.$$

(i) *If $\nu_K(\wp(\mu)) \geq i_2 - pi_1$, then $R[\beta_1, \beta_2]$ is a R-Hopf algebra contained in $(RC_p^2)^*$ with $\mathrm{disc}(R[\beta_1, \beta_2]) = (\pi^{p^2(p-1)(i_1+i_2)})$. The algebra structure of $R[\beta_1, \beta_2]$ is determined by the equations*

$$\beta_1^p = \pi^{(p-1)i_1}\beta_1 - \pi^{pi_1 - i_2}\wp(\mu)\beta_2 \quad \text{and} \quad \beta_2^p = \pi^{(p-1)i_2}\beta_2.$$

The coalgebra structure of $R[\beta_1, \beta_2]$ is determined on the generators, β_r, $r = 1, 2$, by counit $\varepsilon(\beta_r) = 0$, comultiplication

$$\Delta(\beta_r) = \beta_r \otimes 1 + 1 \otimes \beta_r,$$

and antipode $S(\beta_r) = -\beta_r$. Notably, the generators β_1, β_2 are primitive.

(ii) *Let $\beta_1' = \pi^{i_1}(\xi_{1,0} - \mu'\xi_{0,1})$ for some $\mu' \in K$ satisfying*

$$\nu_K(\wp(\mu')) \geq i_2 - pi_1.$$

Then $R[\beta_1', \beta_2]$ is a Hopf algebra, and $R[\beta_1', \beta_2] = R[\beta_1, \beta_2]$ if and only if $\nu_K(\mu' - \mu) \geq i_2 - i_1$,

Remark 3.3. There are only minor differences in notation between the description here and that in [Koc16, Corollary 6.5], which classifies all Hopf orders in $(KC_p^2)^*$.

Proof of Proposition 3.2. (i) Check that β_1 and β_1 satisfy the given equations. The valuative condition $\nu_K(\wp(\mu)) \geq i_2 - pi_1$ is equivalent to $\pi^{pi_1 - i_2}\wp(\mu) \in R$, which is equivalent to $\beta_1^p \in R\beta_1 + R\beta_2$. Thus $R[\beta_1, \beta_2]$ has rank p^2 as an R-algebra. The fact that it is a R-Hopf algebra with the claimed structure follows immediately from Lemma 3.1. Regarding the discriminant, abusing notation, there is a short exact sequence

$$R \to R[\pi^{i_2}\xi_{0,1}] \to R[\beta_1, \beta_2] \to R[\pi^{i_1}\xi_{1,0}] \to R,$$

where $R[\pi^{i_2}\xi_{0,1}]$ and $R[\pi^{i_1}\xi_{1,0}]$ are rank p Hopf algebras. Now using Proposition 2.2,

$$\mathrm{disc}(R[\beta_1, \beta_2]) = \mathrm{disc}(R[\pi^{i_2}\xi_{0,1}])^p \mathrm{disc}(R[\pi^{i_1}\xi_{1,0}])^p = (\pi^{p^2(p-1)(i_1+i_2)})$$

by [Chi00, Corollary (22.17)].

(ii) One has $\beta_1' - \beta_1 = \pi^{i_1}\mu'\xi_{0,1} - \pi^{i_1}\mu\xi_{0,1} = \pi^{i_1}\xi_{0,1}(\mu' - \mu)$ is in $R[\pi^{i_2}\xi_{0,1}]$ if and only if $\nu_K(\mu' - \mu) \geq i_2 - i_1$. The result follows. □

Let x, y be indeterminates, and let $(1+x)^y = \sum_{i=0}^{\infty} \binom{y}{i} x^i \in \mathbb{Q}[y][[x]]$ be the binomial series with $\binom{y}{i} = (y(y-1)\cdots(y-i-1))/i! \in \mathbb{Q}[y]$. We employ the following truncation,

$$(1+x)^{[y]} = \sum_{i=0}^{p-1} \binom{y}{i} x^i,$$

which has coefficients in $\mathbb{Z}_{(p)}$, the integers localized at p. Setting $x = \sigma_1 - 1$ and $y = \mu \in K$ yields $\sigma_1^{[\mu]} = \sum_{i=0}^{p-1} \binom{\mu}{i}(\sigma_1 - 1)^i \in K\langle\sigma_1\rangle$.

Proposition 3.4. *Given $i_1, i_2 \geq 0$, let*

$$\mathcal{H} = R\left[\frac{\sigma_1 - 1}{\pi^{i_1}}, \frac{\sigma_2\sigma_1^{[\mu]} - 1}{\pi^{i_2}}\right].$$

If $\nu_K(\wp(\mu)) \geq i_2 - pi_1$, then $\mathcal{H}$ is a Hopf order in KC_p^2 with $\operatorname{disc}(\mathcal{H}^*) = (\pi^{p^2(p-1)(i_1+i_2)})$.

Remark 3.5. We translate between the descriptions in [Tos10] and Proposition 3.4. First, since [Tos10] treats both groups of order p^2, we need to point out that the elementary abelian case is the case $j = 0$. Furthermore, there is an μ in [Tos10] and a μ here. Naturally, they are different.

[Tos10, Proposition 3.24]	Our notation
μ	π^{i_1}
λ	π^{i_2}
a	$\mu\pi^{i_1}$
$F(T)$	$(1 + \pi^{i_1}T)^{[\mu]}$
$a \in (R/\lambda R)^{F-\mu^{p-1}}$	$\nu_K(\wp(\mu)) \geq i_2 - pi_1$
$pa - j\mu = pa^p/\mu^{p-1} \in R/\lambda^p R$	$-p\wp(\mu) - j \in P^{pi_2 - i_1}$

Since $j = 0$ and $\operatorname{char}(K) = p$, the last statement imposes no restriction.

Under the further identifications,

T_1	$(\sigma_1 - 1)/\pi^{i_1}$
$F(T_1)$	$\sigma_1^{[\mu]}$
T_2	$(\sigma_2^{-1} - \sigma_1^{[\mu]})/\pi^{i_2}$,

the statement of [Tos10, Lemma-Definition 3.9] becomes

$$\mathcal{E}^{(\mu,\lambda;F,0)} = \operatorname{Spec}\left(R\left[\frac{\sigma_1 - 1}{\pi^{i_1}}, \frac{\sigma_2^{-1} - \sigma_1^{[\mu]}}{\pi^{i_2}}\right]\right).$$

Since the group ring $R[\sigma_1, \sigma_2]$ lies in every Hopf order, σ_2 is available, and we may multiply $(\sigma_2^{-1} - \sigma_1^{[\mu]})/\pi^{i_2}$ by $-\sigma_2$ to arrive at the description in Proposition 3.4. The fact that every $\mathcal{H}$ in KC_p^2 is described as in Proposition 3.4 can now be seen to follow from [Tos10, Corollary 3.20], as well as from Theorem 4.6.

Proof. We begin by proving the polynomial identity,

$$(1 + x)^{[y]}(1 + x)^{[z]} = (1 + x)^{[y+z]} \in \mathbb{F}_p[x, y, z]/(x^p). \tag{2}$$

The combinatorial Vandermonde identity leads to the identity

$$\binom{y + z}{n} = \sum_{i=0}^{n} \binom{y}{i}\binom{z}{n - i}$$

in $\mathbb{Q}[x,y]$, which leads to the power series identity

$$(1+x)^y(1+x)^z = (1+x)^{y+z}$$

in $\mathbb{Q}[y,z][[x]]$. Reduce both sides modulo (x^p), and we have

$$(1+x)^{[y]}(1+x)^{[z]} = (1+x)^{[y+z]}$$

in $\mathbb{Q}[x,y,z]/(x^p)$. Note that the coefficients lie in $\mathbb{Z}_{(p)}$. We may reduce modulo p.

We would like now to use [Chi00, Proposition (31.2)] to prove that $\mathcal{H}$ is a Hopf order. To do so, we require that $\sigma^{[\mu]}$ is a unit in $A = R[Z]$ where $Z = (\sigma_1 - 1)/\pi^{i_1}$. Since $x = (\sigma_1 - 1) \in K\langle\sigma_1\rangle$ satisfies $x^p = 0$, we may use (2) to find that $\sigma_1^{[\mu]}\sigma_1^{[-\mu]} = \sigma_1^{[0]} = 1$. Thus it is a unit in $R[Z]$, if $\sigma_1^{[\pm\mu]} = \sum_{r=0}^{p-1}\binom{\pm\mu}{r}\pi^{ri_1}Z^r \in R[Z]$, or equivalently, if $\binom{\pm\mu}{r}\pi^{ri_1} \in R$ for $0 \le r < p$. For $\mu \in R$, this is clear. So assume $\nu_K(\mu) < 0$. Here $p\nu_K(\mu) = \nu_K(\wp(\mu)) \ge i_2 - pi_1 \ge -pi_1$, and thus $\nu_K(\pm\mu) \ge -i_1$, which means that $\nu_K(\binom{\pm\mu}{r}\pi^{ri_1}) \ge 0$.

We are now ready to use [Chi00, Proposition (31.2)]. As we do so, it is important to observe that [Chi00, Proposition (31.2)] holds regardless of characteristic. One simply needs to understand that in [Chi00, Proposition (31.1)], $e' = \nu_K(p)/(p-1) = \infty$ because $\mathrm{char}(K) = p$. It states that $\mathcal{H}$ is a Hopf order if the following two conditions hold.

(a) $(\sigma_2\sigma_1^{[\mu]})^p - 1 \in \pi^{pi_2}A$,
(b) $\Delta(\sigma_1^{[\mu]}) \equiv \sigma_1^{[\mu]} \otimes \sigma_1^{[\mu]} \pmod{\pi^{i_2}(A\otimes A)}$.

It is easy to see that because $\mathrm{char}(K) = p$, $(\sigma_2\sigma_1^{[\mu]})^p = 1$ and condition (a) holds. Consider condition (b): Let

$$X = (\sigma_1 - 1)/\pi^{i_1} \otimes 1 \quad \text{and} \quad Y = 1 \otimes (\sigma_1 - 1)/\pi^{i_1},$$

so that $A \otimes A = R[X,Y]$. Since Δ is an algebra map and

$$\Delta(\sigma_1) = \sigma_1 \otimes \sigma_1 = (1+\pi^{i_1}X)(1+\pi^{i_2}Y),$$

condition (b) can be restated as

$$((1+\pi^{i_1}X)(1+\pi^{i_2}Y))^{[\mu]} \equiv (1+\pi^{i_1}X)^{[\mu]}(1+\pi^{i_2}Y)^{[\mu]} \pmod{\pi^{i_2}R[X,Y]}.$$

Observe that $X^p = Y^p = 0$. To analyze this further we need from [ByE05, Lemma 2.2]:

$$(1+x+y+xy)^{[z]} = (1+x)^{[z]}(1+y)^{[z]}(1+\wp(z)Q(x,y)) \in \mathbb{F}_p[x,y,z]/(x^p,y^p),$$

where $Q(x,y) = ((x+y+xy)^p - x^p - y^p - (xy)^p)/p \in (x,y)^p \subset \mathbb{Z}[x,y]$. For the convenience of the reader we replicate the argument here: First observe that for $p \le i < 2p-1$, we have the polynomial identity

$$p\binom{z}{i} \equiv p\binom{z}{p}\binom{z}{i-p} \equiv -\wp(z)\binom{z}{i-p} \bmod p\mathbb{Z}_{(p)}[z]$$

where $\wp(z) = z^p - z$ and $\mathbb{Z}_{(p)}$ denotes the integers localized at p. Observe that within the power series ring $\mathbb{Q}[z][[x,y]]$ we have the identity

$$((1+x)(1+y))^z = (1+x)^z(1+y)^z,$$

which we reduce modulo (x^p, y^p). The result is $(1+w)^z = (1+x)^{[z]}(1+y)^{[z]}$ where $w = x + y + xy$ lies in the ideal (x,y). Since $(x,y)^{2p-1} \subseteq (x^p, y^p)$ we have the identity $(1+x)^{[z]}(1+y)^{[z]} = \sum_{i=0}^{2p-2} \binom{z}{i} w^i$ in $\mathbb{Q}[x,y,z]/(x^p,y^p)$. Observe that $w^p = pQ(x,y)$. Therefore

$$\sum_{i=0}^{2p-2} \binom{z}{i} w^i = (1+w)^{[z]} + Q(x,y) \sum_{i=p}^{2p-2} p\binom{z}{i} w^{i-p}.$$

Since the coefficients lie in $\mathbb{Z}_{(p)}$, we find, upon reducing modulo p, that $(1+x)^{[z]}(1+y)^{[z]} = (1+w)^{[z]}(1-\wp(z)Q(x,y))$ in $\mathbb{F}_p[x,y,z]/(x^p,y^p)$. Since $Q(x,y) \in (x,y)^p$, $Q(x,y)^2 = 0$ and the polynomial identity is established.

From this polynomial identity, we see that the second condition is the requirement that

$$\begin{aligned}(1+\pi^{i_1}X)^{[\mu]}(1+\pi^{i_2}Y)^{[\mu]}&(1+\wp(\mu)Q(\pi^{i_1}X,\pi^{i_1}Y)) \\ &\equiv (1+\pi^{i_1}X)^{[\mu]}(1+\pi^{i_2}Y)^{[\mu]} \pmod{\pi^{i_2}R[X,Y]}.\end{aligned}$$

But $(1+\pi^{i_1}X)^{[\mu]}$ and $(1+\pi^{i_2}Y)^{[\mu]}$ are both units in $R[X,Y]$, which means that we need $1+\wp(\mu)Q(\pi^{i_1}X,\pi^{i_1}Y) \equiv 1 \pmod{\pi^{i_2}R[X,Y]}$. This follows from $\pi^{pi_1}\wp(\mu) \in \pi^{i_2}R$, which is equivalent to $\nu_K(\wp(\mu)) \geq i_2 - pi_1$, since $Q(\pi^{i_1}X,\pi^{i_1}Y) \in \pi^{pi_1}R[X,Y]$.

The Hopf order $\mathcal{H}$ now sits within the short exact sequence

$$R \to \mathcal{H}_{i_1} \to \mathcal{H} \to \mathcal{H}_{i_2} \to R,$$

with its dual $\mathcal{H}^*$ sitting within $R \to \mathcal{H}^*_{i_2} \to \mathcal{H}^* \to \mathcal{H}^*_{i_1} \to R$. We may use the computations of $\operatorname{disc}(\mathcal{H}^*_{i_r})$ from Corollary 2.2 and [Chi00, Propositions (5.6), (22.15) and Corollary (22.17)] to determine $\operatorname{disc}(\mathcal{H}^*)$ in a similar fashion to Corollary 3.2. □

Theorem 3.6. *Let $\mathcal{H}$ be as in Proposition 3.4, then $\mathcal{H}^* = R[\beta_1,\beta_2]$ as in Proposition 3.2.*

Proof. Based upon Propositions 3.2 and 3.4,

$$\operatorname{disc}(R[\beta_1,\beta_2]) = \operatorname{disc}(\mathcal{H}^*) = (\pi^{p^2(p-1)(i_1+i_2)}).$$

Therefore we only need to prove $\beta_1, \beta_2 \in \mathcal{H}^*$, so that $R[\beta_1,\beta_2] \subseteq \mathcal{H}^*$. The set $\{\alpha_{a,b}\}_{a,b=0}^{p-1}$ where $\alpha_{a,b} = (\sigma_1-1)^a(\sigma_2\sigma_1^{[\mu]}-1)^b/\pi^{ai_1+bi_2}$ is an R-basis for $\mathcal{H}$. So for each $r = 1,2$, we need to show $\langle \beta_r, \alpha_{a,b}\rangle \in R$ for all $0 \leq a,b < p$. The effects of $\xi_{1,0}$ and $\xi_{0,1}$ on $\alpha_{a,b}$ are determined modulo $((\sigma_1-1),(\sigma_2-1))^2$. So to assist us in our analysis, we let $\sigma_1 = 1+x$ and $\sigma_2 = 1+y$. Observe that $(\sigma_2\sigma_1^{[\mu]} - 1) \equiv y + \mu x \pmod{(x,y)^2}$. Thus $\pi^{ai_1+bi_2}\alpha_{a,b} \equiv x^a(y+\mu x)^b \pmod{(x,y)^2}$. Using $\langle \xi_{1,0}, x^r y^s\rangle = \delta_{r,1}\delta_{s,0}$ and $\langle \xi_{0,1}, x^r y^s\rangle = \delta_{r,0}\delta_{s,1}$, we have

$$\langle \xi_{1,0}, \pi^{ai_1+bi_2}\alpha_{a,b}\rangle = \begin{cases} 1 & a=1, b=0, \\ \mu & a=0, b=1, \\ 0 & \text{else}, \end{cases}$$

$$\langle \xi_{0,1}, \pi^{ai_1+bi_2}\alpha_{a,b}\rangle = \begin{cases} 0 & a=1, b=0, \\ 1 & a=0, b=1, \\ 0 & \text{else}. \end{cases}$$

Therefore $\langle \beta_1, \alpha_{a,b}\rangle = \delta_{a,1}\delta_{b,0}$ and $\langle \beta_2, \alpha_{a,b}\rangle = \delta_{a,0}\delta_{b,1}$. □

In the next section, we will prove that the Hopf orders described in Propositions 3.2 and 3.4 constitute all possible Hopf orders. Before we do so, we make an observation: Based upon (2), if for some $t \in \mathbb{F}_p$, we set $\mu' = \mu + t$ and $\sigma_2' = \sigma_2\sigma_1^{-t}$, then $\sigma_2'\sigma_1^{[\mu']} = \sigma_2\sigma_1^{[\mu]}$. Based upon Theorem 3.6 and Proposition 3.2(ii), if $\mu' \in \mu + P^{i_2-i_1}$, then

$$R\left[\frac{\sigma_1 - 1}{\pi^{i_1}}, \frac{\sigma_2\sigma_1^{[\mu']} - 1}{\pi^{i_2}}\right] = R\left[\frac{\sigma_1 - 1}{\pi^{i_1}}, \frac{\sigma_2\sigma_1^{[\mu]} - 1}{\pi^{i_2}}\right].$$

Together these mean that given any Hopf order $\mathcal{H}$, described in Proposition 3.4, we may replace μ in the description of $\mathcal{H}$ with any other coset representative for $\mu + \mathbb{F}_p + P^{i_2-i_1}$ in the additive group $K/(\mathbb{F}_p + P^{i_2-i_1})$, as long as we compensate (if necessary) by replacing σ_2 with σ_2', as above. In particular, this means that when we are given a Hopf order $\mathcal{H}$ in Proposition 3.4, we may assume, without loss of generality, the following convention.

Convention 1. $\mu \in K$ is an element of largest valuation in $\mu + \mathbb{F}_p + P^{i_2-i_1}$.

Under this convention, if $\mu \in \mathbb{F}_p + P^{i_2-i_1}$, then $\mu = 0$.

Remark 3.7. Under Convention 1,

$$\nu_K(\wp(\mu)) = \begin{cases} \nu_K(\mu) & \text{for } \nu_K(\mu) \geq 0, \\ p\nu_K(\mu) & \text{for } \nu_K(\mu) \leq 0. \end{cases}$$

So, without loss of generality, the Hopf orders described in Propositions 3.2 and 3.4 may be assumed to satisfy $\mu = 0$ or

$$\max\{i_2 - pi_1, i_2/p - i_1\} \leq \nu_K(\mu) < i_2 - i_1.$$

Observe that $i_2 - pi_1 = i_2/p - i_1$ precisely when $i_2 - pi_1 = i_2/p - i_1 = 0$. If we ignore $\mu = 0$, and plot the possible values of $(x, y, z) = (i_1, i_2, \nu_K(\mu))$ on a 3-dimensional graph, they appear within a triangular cone formed by the planes:

$$x - y + z = 0, \quad px - y + pz = 0, \quad px - y + z = 0.$$

To aid further visualization, note that since $i_1, i_2 \geq 0$, this cone projects orthogonally onto the first quadrant of the $z = 0$ plane, which we refer to as the xy-plane. Henceforth, when we refer to a point in the xy-plane, it is to a point (x, y) with $x, y \geq 0$ without reference to the value of z. The cone's cross-section by the xy-plane is the region bound between $y = x$ and $y = px$ (in center in Figure 1). The cone lies wholly above the xy-plane for (x, y) above $y = px$. The cone lies wholly below the xy-plane for (x, y) below $y = x$. Consider two further cross sections parallel to the xy-plane: When $z > 0$, this cross section is bound between $y = x + z$ and $y = px + z$ (on the left in Figure 1). For $z < 0$ the cross section is bound between $y = x + z$ and $y = px + pz$ (on the right in Figure 1).

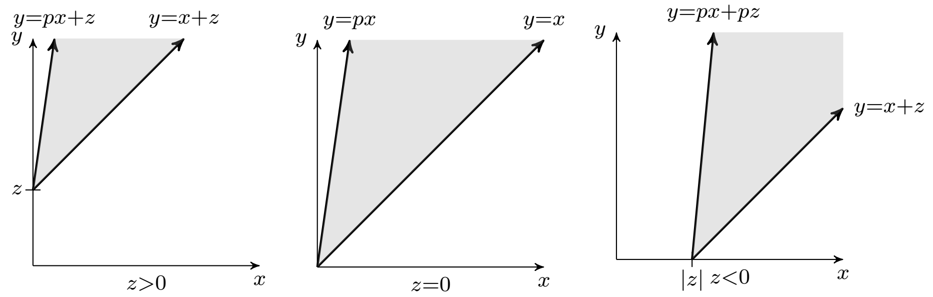

FIGURE 1. Cross-sections parallel to the xy-plane

For another perspective on these points, assume $x = i_1 > 0$, and set $\bar{y} = y/x$, $\bar{z} = z/x$. Each point with $x > 0$ yields a point $(\bar{y}, \bar{z})$ that appears in Figure 2.

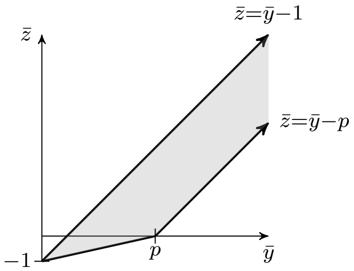

FIGURE 2. Plot of $(\bar{y}, \bar{z}) = (y/x, z/x)$ for $x = i_1 > 0$

4. Classification of Hopf orders in KC_p^2

In this section we classify the Hopf orders in KC_p^2 by classifying the models of $\mu_{p,K}^2$ represented by them. Were we to attack this problem directly by classifying all extensions of a model of $\mu_{p,K}$ by another model of $\mu_{p,K}$, we would be led to the methods of Sekiguchi and Suwa, as in [Tos10]. Motivated by the fact that models of the constant group scheme C_p can be embedded in $\mathbb{G}_a$, the additive group scheme over R, while models of $\mu_{p,K}$ are not all contained in a smooth group scheme of dimension 1, we attack this classification indirectly by studying extensions of group schemes represented by the duals of Hopf orders in KC_p. We do this using the cohomological approach of Greither, closely following [Gre92, Part 1]. Recall $C_p^2 = \langle \sigma_1, \sigma_2 \rangle$, and let $\mathcal{H}$ be a Hopf order in KC_p^2. Let $C_p^2 \to C_p^2/\langle \sigma_1 \rangle$ denote the canonical surjection with $C_p^2/\langle\sigma_1\rangle \cong \langle \bar\sigma_2 \rangle$ where $\bar\sigma_2 = \sigma_2\langle\sigma_1\rangle$. By [Chi00, (5.3) Proposition], there exists a short exact sequence

$$R \to \mathcal{H}_{i_1} \to \mathcal{H} \to \mathcal{H}_{i_2} \to R, \tag{3}$$

where, as described in Theorem 2.3,

$$\mathcal{H}_{i_1} = R[(\sigma_1 - 1)/\pi^{i_1}] \quad \text{and} \quad \mathcal{H}_{i_2} = R[(\bar\sigma_2 - 1)/\pi^{i_2}],$$

for some $i_1, i_2 \geq 0$. Motivated by the observation above, we dualize (3) to obtain the short exact sequence

$$R \to \mathcal{H}_{i_2}^* \to \mathcal{H}^* \to \mathcal{H}_{i_1}^* \to R, \tag{4}$$

with $\mathcal{H}_{i_1}^*$ and $\mathcal{H}_{i_2}^*$ as in Proposition 2.2. Now we follow [Gre92] and translate into the language of group schemes. Let

$$\mathbb{D}_{i_1}^* = \text{Spec } \mathcal{H}_{i_1}^*, \quad \mathbb{D}^* = \text{Spec } \mathcal{H}^*, \quad \text{and} \quad \mathbb{D}_{i_2}^* = \text{Spec } \mathcal{H}_{i_2}^*.$$

These group schemes are representable functors from the category of commutative R-algebras to the category of abelian groups. Classifying Hopf orders $\mathcal{H}$ in (3) or $\mathcal{H}^*$ in (4) is the same as classifying finite group schemes $\mathbb{D}^*$ that fit into the short exact sequence of group schemes

$$0 \to \mathbb{D}_{i_1}^* \to \mathbb{D}^* \to \mathbb{D}_{i_2}^* \to 0, \tag{5}$$

and which are represented by a Hopf order in $(KC_p^2)^*$. In other words, our goal is to compute the subgroup of generically trivial extensions within the full extension group.

4.1. Background. We are working in the category of sheaves of abelian groups in the faithfully flat topology. By [Mil80, II Theorem 2.15(e)], this is an abelian category. By [Mil80, III Proposition 1.1], it contains enough injectives. Thus we let Ext^r, $r \geq 0$ denote the rth right derived functor of Hom in the category of sheaves, and observe that development of Ext^r using injective resolutions can be found in [Lan02, XX, §6]. Indeed, $\text{Ext}^1(\mathbb{D}_{i_2}^*, \mathbb{D}_{i_1}^*)$ is an abelian group, and Ext^1 can be explicitly calculated using any injective presentation, as follows: Let

$$0 \to \mathbb{D}_{i_1}^* \xrightarrow{\epsilon} \mathbb{I} \xrightarrow{s} \mathbb{S} \to 0, \quad \mathbb{S} = \mathbb{I}/\epsilon(\mathbb{D}_{i_1}^*).$$

be an injective presentation of $\mathbb{D}_{i_1}^*$. Then from the long exact sequence, one obtains the exact sequence

$$\text{Hom}(\mathbb{D}_{i_2}^*, \mathbb{I}) \xrightarrow{s} \text{Hom}(\mathbb{D}_{i_2}^*, \mathbb{S}) \xrightarrow{\delta} \text{Ext}^1(\mathbb{D}_{i_2}^*, \mathbb{D}_{i_1}^*) \to \text{Ext}^1(\mathbb{D}_{i_2}^*, \mathbb{I}),$$

with δ the connecting homomorphism [Lan02, XX Theorem 6.1]. By [Lan02, XX Theorem 6.1(v)], $\mathrm{Ext}^1(\mathbb{D}_{i_2}^*, \mathbb{I}) = 0$, thus $\mathrm{Ext}^1(\mathbb{D}_{i_2}^*, \mathbb{D}_{i_1}^*) \cong \mathrm{Ext}^{\epsilon}(\mathbb{D}_{i_2}^*, \mathbb{D}_{i_1}^*)$, where

$$\mathrm{Ext}^{\epsilon}(\mathbb{D}_{i_2}^*, \mathbb{D}_{i_1}^*) = \mathrm{coker}(s : \mathrm{Hom}(\mathbb{D}_{i_2}^*, \mathbb{I}) \to \mathrm{Hom}(\mathbb{D}_{i_2}^*, \mathbb{S})).$$

In view of [HS71, III, Theorem 2.4 (dual version)] and [HS71, III, §3, p. 94], we may also identify $\mathrm{Ext}^1(\mathbb{D}_{i_2}^*, \mathbb{D}_{i_1}^*)$ with $\mathrm{E}(\mathbb{D}_{i_2}^*, \mathbb{D}_{i_1}^*)$, the equivalence classes of short exact sequences with $[\mathbb{D}^*] \in \mathrm{E}(\mathbb{D}_{i_2}^*, \mathbb{D}_{i_1}^*)$ represented by (5). As a result of this identification, the group operation in $\mathrm{Ext}^1(\mathbb{D}_{i_2}^*, \mathbb{D}_{i_1}^*)$ is the Baer sum, and the connecting homomorphism δ is given by a pullback construction that produces a class in $\mathrm{E}(\mathbb{D}_{i_2}^*, \mathbb{D}_{i_1}^*)$ and thus an element in $\mathrm{Ext}^1(\mathbb{D}_{i_2}^*, \mathbb{D}_{i_1}^*)$. Recall however that Ext^1 classifies extensions of sheaves. Given two group schemes, Ext^1 obtains all extensions as commutative sheaves. However, because in our situation $\mathbb{D}_{i_1}^*$ is an affine group scheme, the extensions classified by $\mathrm{Ext}^1(\mathbb{D}_{i_2}^*, \mathbb{D}_{i_1}^*)$ are representable and thus affine group schemes [Oor66, III, Proposition 17.4].

Remark 4.1. The description of the connecting homomorphism via pullbacks will be used in the proof of Theorem 4.6; we discuss it now for $\delta : \mathrm{Hom}(\mathbb{D}_{i_2}^*, \mathbb{T}) \to \mathrm{Ext}^1(\mathbb{D}_{i_2}^*, \mathbb{D}_{i_1}^*)$ arising from any short exact sequence $0 \to \mathbb{D}_{i_1}^* \xrightarrow{\epsilon} \mathbb{J} \xrightarrow{s} \mathbb{T} \to 0$ (not just an injective presentation): Embed $\mathbb{J}$ into an injective object $\mathbb{I}$. This results in an injective presentation

$$0 \to \mathbb{D}_{i_1}^* \xrightarrow{\epsilon'} \mathbb{I} \xrightarrow{s'} \mathbb{T}' \to 0.$$

There is a canonical injection $\mathbb{T} \to \mathbb{T}'$ which we consider as the inclusion $\mathbb{T} \subseteq \mathbb{T}'$. Let $\delta' : \mathrm{Hom}(\mathbb{D}_{i_2}^*, \mathbb{T}') \to \mathrm{Ext}^1(\mathbb{D}_{i_2}^*, \mathbb{D}_{i_1}^*)$ be the connecting homomorphism, which as discussed above, yields the isomorphism

$$\mathrm{Ext}^{\epsilon'}(\mathbb{D}_{i_2}^*, \mathbb{D}_{i_1}^*) \cong \mathrm{Ext}^1(\mathbb{D}_{i_2}^*, \mathbb{D}_{i_1}^*).$$

There is a commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}(\mathbb{D}_{i_2}^*, \mathbb{J}) \arrow[r] \arrow[d] & \mathrm{Hom}(\mathbb{D}_{i_2}^*, \mathbb{T}) \arrow[r, "\delta"] \arrow[d] & \mathrm{Ext}^1(\mathbb{D}_{i_2}^*, \mathbb{D}_{i_1}^*) \arrow[d, equal] & \\
\mathrm{Hom}(\mathbb{D}_{i_2}^*, \mathbb{I}) \arrow[r] & \mathrm{Hom}(\mathbb{D}_{i_2}^*, \mathbb{T}') \arrow[r, "\delta'"] & \mathrm{Ext}^1(\mathbb{D}_{i_2}^*, \mathbb{D}_{i_1}^*) \arrow[r] & 0
\end{tikzcd}$$

where the left and middle vertical maps are injections. We will now explicitly describe δ, which in general is not a surjection. Let $\beta : \mathbb{D}_{i_2}^* \to \mathbb{T}$ be a homomorphism, and let β' denote its image in $\mathrm{Hom}(\mathbb{D}_{i_2}^*, \mathbb{T}')$. There is a commutative diagram

$$\begin{tikzcd}
\mathbb{D}_{\beta'}^* \arrow[r, "\pi_2"] \arrow[d, "\pi_1"] & \mathbb{I} \arrow[d, "s'"] \\
\mathbb{D}_{i_2}^* \arrow[r, "\beta'"] & \mathbb{T}'
\end{tikzcd}$$

where $\mathbb{D}^*_{\beta'} = \{(x,y) \in \mathbb{D}^*_{i_2} \times \mathbb{I} : \ \beta'(x) = s'(y)\}$ is the pull-back of (β', s'). Of course, this construction should be understood in the functorial sense: $\mathbb{D}^*_{\beta'}(S) = \{(x,y) \in \mathbb{D}^*_{i_2}(S) \times \mathbb{I}(S) : \ \beta'(x) = s'(y)\}$ for every commutative R-algebra S. Since β' arises from β, which has image in $\mathbb{T}$, the image of β' is contained in $\mathbb{T}$ as well. Therefore each y for which $(x,y) \in \mathbb{D}^*_{\beta'}$ must be in $\mathbb{J}$. Thus $\mathbb{D}^*_{\beta'}$ is the pull-back of (β, s), that is, the following diagram commutes:

$$\begin{tikzcd}
\mathbb{D}^*_{\beta'} \arrow[r, "\pi_2"] \arrow[d, "\pi_1"] & \mathbb{J} \arrow[d, "s"] \\
\mathbb{D}^*_{i_2} \arrow[r, "\beta"] & \mathbb{T}
\end{tikzcd}$$

The image of β under δ is the class $[\mathbb{D}^*_{\beta'}] \in \operatorname{Ext}^1(\mathbb{D}^*_{i_2}, \mathbb{D}^*_{i_1})$, which we denote by $[\mathbb{D}^*_{\beta}]$.

4.2. Argument. Our goal is to compute the subgroup of generically trivial extensions, which we denote with a subscript *gt*. For every sheaf $\mathbb{F}$ of abelian groups on the category of commutative R-algebras, we let $K \otimes_R \mathbb{F}$ be the restriction of $\mathbb{F}$ to the category of commutative K-algebras. If $\mathbb{F}$ is represented by the R-Hopf algebra $\mathcal{H}$, then $K \otimes_R \mathbb{F}$ is represented by the K-Hopf algebra $K \otimes_R \mathcal{H}$. If $\mathbb{G}$ is another representable sheaf, then the flatness of K over R implies the existence of a natural map

$$\operatorname{Ext}^1(\mathbb{F}, \mathbb{G}) \to \operatorname{Ext}^1(K \otimes_R \mathbb{F}, K \otimes_R \mathbb{G}).$$

This map is a group homomorphism. Let $\operatorname{Ext}^1_{gt}(\mathbb{F}, \mathbb{G})$ denote its kernel. More generally, for every group-valued functor $\mathbb{E}$ on commutative R-algebras, we will define the functor $\mathbb{E}_{gt}$ by $S \mapsto \ker\big(\mathbb{E}(S) \to \mathbb{E}(K \otimes_R S)\big)$.

Towards determining $\operatorname{Ext}^1_{gt}(\mathbb{D}^*_{i_2}, \mathbb{D}^*_{i_1})$, we recall the motivating observation from the beginning of this section and introduce the following short exact sequence:

$$0 \to \mathbb{D}^*_{i_1} \xrightarrow{\iota_1} \mathbb{G}_a \xrightarrow{\Psi_1} \mathbb{G}_a \to 0, \tag{6}$$

which is a consequence of the following: The polynomial ring $R[x]$ with counit $\varepsilon(x) = 0$, comultiplication $\Delta(x) = x \otimes 1 + 1 \otimes x$ and antipode $S(x) = -x$ represents the additive group scheme $\mathbb{G}_a$. For $i_1 \geq 0$, the R-algebra map $\psi : R[x] \to R[x]$ determined by $\psi(x) = x^p - \pi^{(p-1)i_1}x$ is a homomorphism of Hopf algebras, and so, there exists a homomorphism of R-group schemes $\Psi_1 : \mathbb{G}_a \to \mathbb{G}_a$, defined by $\Psi_1(g)(x) = g(\psi(x))$ for $g \in \mathbb{G}_a$. Given a commutative R-algebra S, and $g \in \mathbb{G}_a(S)$ defined by $g(x) = s \in S$ then $\Psi_1(g) \in \mathbb{G}_a(S)$ is defined by $\Psi_1(g)(x) = g(\psi(x)) = s^p - \pi^{(p-1)i_1}s$. Using Proposition 2.2, we have the isomorphism of R-Hopf algebras, $R[x]/(\psi(x)) \cong \mathcal{H}^*_{i_1}$, and so the kernel of Ψ_1 is the subgroup scheme represented by $\mathcal{H}^*_{i_1}$, namely $\mathbb{D}^*_{i_1}$. Furthermore, Ψ_1 is surjective in the faithfully flat topology: Given $g \in \mathbb{G}_a(S)$ defined by $g(x) = s \in S$, we may let s' be a root of $\psi(x) - s$ in some ring extension of S. Let $S' = S[s']$ with the natural faithfully flat map of S into S'. Then $g' \in \mathbb{G}_a(S')$ defined by $g'(x) = s'$ satisfies

$$\Psi_1(g')(x) = g'(\psi(x)) = \psi(s') = s.$$

Using [Lan02, XX Theorem 6.1], (6) produces the long exact sequence:

$$\mathrm{Hom}(\mathbb{D}^*_{i_2}, \mathbb{G}_a) \xrightarrow{\Psi_1} \mathrm{Hom}(\mathbb{D}^*_{i_2}, \mathbb{G}_a) \overset{\omega}{\to} \mathrm{Ext}^1(\mathbb{D}^*_{i_2}, \mathbb{D}^*_{i_1}) \overset{\iota_1}{\to} \mathrm{Ext}^1(\mathbb{D}^*_{i_2}, \mathbb{G}_a),$$

with connecting homomorphism ω, which induces the map ρ in the exact sequence

$$0 \to \mathrm{coker}(\Psi_1 \colon \mathrm{Hom}(\mathbb{D}^*_{i_2}, \mathbb{G}_a)^{\circlearrowleft}) \overset{\rho}{\to} \mathrm{Ext}^1(\mathbb{D}^*_{i_2}, \mathbb{D}^*_{i_1}) \overset{\iota_1}{\to} \mathrm{Ext}^1(\mathbb{D}^*_{i_2}, \mathbb{G}_a).$$

Tensoring with K and considering kernels, which we indicate with gt, results in the following commutative diagram with exact rows and columns:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] \\
0 \arrow[r] & \mathrm{coker}(\Psi_1 \colon \mathrm{Hom}(\mathbb{D}^*_{i_2}, \mathbb{G}_a)^{\circlearrowleft})_{gt} \arrow[r] \arrow[d] & \mathrm{Ext}^1_{gt}(\mathbb{D}^*_{i_2}, \mathbb{D}^*_{i_1}) \arrow[r] \arrow[d] & \mathrm{Ext}^1_{gt}(\mathbb{D}^*_{i_2}, \mathbb{G}_a) \arrow[d] \\
0 \arrow[r] & \mathrm{coker}(\Psi_1 \colon \mathrm{Hom}(\mathbb{D}^*_{i_2}, \mathbb{G}_a)^{\circlearrowleft}) \arrow[r] \arrow[d] & \mathrm{Ext}^1(\mathbb{D}^*_{i_2}, \mathbb{D}^*_{i_1}) \arrow[r] \arrow[d] & \mathrm{Ext}^1(\mathbb{D}^*_{i_2}, \mathbb{G}_a) \arrow[d] \\
0 \arrow[r] & \mathrm{coker}(\Psi_1 \colon \mathrm{Hom}(\mathbb{D}^*_K, \mathbb{G}_K)^{\circlearrowleft}) \arrow[r] & \mathrm{Ext}^1(\mathbb{D}^*_K, \mathbb{G}_K) \arrow[r] & \mathrm{Ext}^1(\mathbb{D}^*_K, \mathbb{G}_K),
\end{tikzcd} \tag{7}$$

where $\mathbb{D}^*_K = K \otimes_R \mathbb{D}^*_{i_2}$ and $\mathbb{G}_K = K \otimes_R \mathbb{G}_a$. Exactness in the top exact sequence is justified by a diagram chase.

Outline. Having introduced commutative diagram (7), we are prepared to outline the remainder of the section. In Proposition 4.2, we analyze a spectral sequence in order to conclude that $\mathrm{Ext}^1(\mathbb{D}^*_{i_2}, \mathbb{G}_a) \cong \mathrm{H}^2_0(\mathbb{D}^*_{i_2}, \mathbb{G}_a)$. This is important as it allows us to compute $\mathrm{Ext}^1(\mathbb{D}^*_{i_2}, \mathbb{G}_a)$ in terms of cocycles modulo coboundaries, something we do in Proposition 4.3, thereby proving that $\mathrm{Ext}^1_{gt}(\mathbb{D}^*_{i_2}, \mathbb{G}_a)$ is trivial. This means, using the commutative diagram, that we can conclude, as we do in Corollary 4.4, that

$$\mathrm{Ext}^1_{gt}(\mathbb{D}^*_{i_2}, \mathbb{D}^*_{i_1}) \cong \mathrm{coker}(\Psi_1 \colon \mathrm{Hom}(\mathbb{D}^*_{i_2}, \mathbb{G}_a)^{\circlearrowleft})_{gt}.$$

In Proposition 4.5, we identify this cokernel with the additive subgroup of those cosets in $K/(\mathbb{F}_p + P^{i_2 - i_1})$ represented by $\mu \in K$ satisfying

$$\nu_K(\wp(\mu)) \geq i_2 - pi_1.$$

All this sets the stage for Theorem 4.6, where we use (6) together with the usual pullback construction to identify each element of this cokernel, represented by an explicit coset in $K/(\mathbb{F}_p + P^{i_2 - i_1})$, with an explicit extension (5) of group schemes.

The first step is a characteristic p version of [Gre92, Theorem 2.1].

Proposition 4.2. $\mathrm{Ext}^1(\mathbb{D}^*_{i_2}, \mathbb{G}_a) \cong \mathrm{H}^2_0(\mathbb{D}^*_{i_2}, \mathbb{G}_a)$.

Proof. Let $\mathbb{G}$ be any R-group scheme. For $q \geq 0$, let $\mathfrak{H}^q(\mathbb{G})$ denote the presheaf $A \mapsto \mathrm{H}^q(A, \mathbb{G}_A)$ where H^q is the qth cohomology group of the base-extended sheaf $\mathbb{G}_A$, see [Mil80, III, §2]. Specializing to $\mathbb{G} = \mathbb{G}_a$, [DG70, III, §6, 2.3 Proposition] provides a first quadrant spectral sequence for $r, q \geq 0$, $\mathrm{H}_0^{r+1}(\mathbb{D}_{i_2}^*, \mathfrak{H}^q(\mathbb{G}_a))$ which converges to $\mathrm{Ext}^{r+q}(\mathbb{D}_{i_2}^*, \mathbb{G}_a)$. Using [Mil80, Appendix B], one gets the long exact sequence

$$0 \to \mathrm{H}_0^2(\mathbb{D}_{i_2}^*, \mathfrak{H}^0(\mathbb{G}_a)) \to \mathrm{Ext}^1(\mathbb{D}_{i_2}^*, \mathbb{G}_a) \to \mathrm{H}_0^1(\mathbb{D}_{i_2}^*, \mathfrak{H}^1(\mathbb{G}_a)) \to \mathrm{H}_0^3(\mathbb{D}_{i_2}^*, \mathfrak{H}^0(\mathbb{G}_a)).$$

By [Wat79, p, 139, Exercise 10], $\mathfrak{H}^1(\mathbb{G}_a) = 0$, and $\mathrm{H}_0^1(\mathbb{D}_{i_2}^*, \mathfrak{H}^1\mathbb{G}_a)) = 0$. The result follows. □

Our next result is the characteristic p analog of [Gre92, I §3].

Proposition 4.3. $\mathrm{Ext}_{gt}^1(\mathbb{D}_{i_2}^*, \mathbb{G}_a) = 0$.

Proof. For $r \geq 0$, let $(\mathbb{D}_{i_2}^*)^r$ denote the product. Let $\mathbb{X}$ be an R-presheaf of abelian groups in the faithfully flat topology, and let $\mathrm{Mor}_0((\mathbb{D}_{i_2}^*)^r, \mathbb{X})$ denote the collection of all morphisms $f : (\mathbb{D}_{i_2}^*)^r \to \mathbb{X}$ which satisfy $f_S(0, 0, \ldots, 0) = 0$ for each commutative R-algebra S. Here each 0 in the r-tuple $(0, 0, \ldots, 0)$ is the identity element $\lambda_S \epsilon_{\mathcal{H}_{i_2}^*} \in \mathbb{D}_{i_2}^*(S)$, where $\lambda_S : R \to S$ is the R-algebra structure map of S. For the case $\mathbb{X} = \mathbb{G}_a$, by Yoneda's Lemma, morphisms in $\mathrm{Mor}_0((\mathbb{D}_{i_2}^*)^r, \mathbb{G}_a)$ correspond to elements $a \in \mathcal{H}_{i_2}^* \otimes \mathcal{H}_{i_2}^* \otimes \cdots \otimes \mathcal{H}_{i_2}^*$ which are in $\ker(\epsilon_{\mathcal{H}_{i_2}^*} \otimes \epsilon_{\mathcal{H}_{i_2}^*} \otimes \cdots \otimes \epsilon_{\mathcal{H}_{i_2}^*})$. For $r \geq 1$, we define a complex

$$\mathrm{Mor}_0((\mathbb{D}_{i_2}^*)^{r-1}, \mathbb{X}) \xrightarrow{\partial_{r-1}} \mathrm{Mor}_0((\mathbb{D}_{i_2}^*)^r, \mathbb{X}) \xrightarrow{\partial_r} \mathrm{Mor}_0((\mathbb{D}_{i_2}^*)^{r+1}, \mathbb{X}) \xrightarrow{\partial_{r+1}} .$$

For small r the boundary maps, for $x, y, z \in \mathbb{D}_{i_2}^*(S)$, are defined as $\partial_0 = 0$,

$$(\partial_1 g)_S(x, y) = g_S(x) - g_S(x + y) + g_S(y),$$
$$(\partial_2 f)_S(x, y, z) = f_S(x, y) - f_S(x, y + z) + f_S(x + y, z) - f_S(y, z).$$

For $r \geq 0$, let $\mathrm{H}_0^r(\mathbb{D}_{i_2}^*, \mathbb{X})$ denote the rth cohomology group of this complex. Thus

$$\mathrm{H}_0^2(\mathbb{D}_{i_2}^*, \mathbb{G}_a) = C_0^2(\mathbb{D}_{i_2}^*, \mathbb{G}_a)/B_0^2(\mathbb{D}_{i_2}^*, \mathbb{G}_a)$$

with cocycles $C_0^2(\mathbb{D}_{i_2}^*, \mathbb{G}_a) = \{f \in \mathrm{Mor}_0(\mathbb{D}_{i_2}^* \times \mathbb{D}_{i_2}^*, \mathbb{G}_a) : \partial_2(f) = 0\}$ and coboundaries $B_0^2(\mathbb{D}_{i_2}^*, \mathbb{G}_a) = \{\partial_1(g) : g \in \mathrm{Mor}_0(\mathbb{D}_{i_2}^*, \mathbb{G}_a)\}$. Since $\mathbb{G}_a$ is represented by $R[x]$, by Yoneda's Lemma, the morphisms $f \in \mathrm{Mor}_0(\mathbb{D}_{i_2}^* \times \mathbb{D}_{i_2}^*, \mathbb{G}_a)$ correspond bijectively to elements of $\mathcal{H}_{i_2}^* \otimes \mathcal{H}_{i_2}^*$ that lie in the augmentation ideal, the kernel of $\epsilon_{\mathcal{H}_{i_2}^*} \otimes \epsilon_{\mathcal{H}_{i_2}^*}$. Moreover $\delta_2(f) = 0$ means that the corresponding element is in the kernel of

$$1 \otimes \mathrm{id} \otimes \mathrm{id} - \Delta \otimes \mathrm{id} + \mathrm{id} \otimes \Delta - \mathrm{id} \otimes \mathrm{id} \otimes 1. \tag{8}$$

Similarly, morphisms $g \in \mathrm{Mor}_0(\mathbb{D}_{i_2}^*, \mathbb{G}_a)$ correspond to elements $a \in \mathcal{H}_{i_2}^*$ that lie in the kernel of $\epsilon_{\mathcal{H}_{i_2}^*}$ with $\delta_1(g)$ corresponding to its image under $1 \otimes \mathrm{id} - \Delta + \mathrm{id} \otimes 1$, namely

$$\xi_0 \otimes a - \Delta(a) + a \otimes \xi_0 \in \mathcal{H}_{i_2}^* \otimes \mathcal{H}_{i_2}^*.$$

Let $C_p = \langle \sigma \rangle$, and recall from proof of Lemma 2.1 that $\{\xi_r\}_{r=0}^{p-1}$ is the R-basis for RC_p^* dual to $\{(\sigma-1)^s\}_{s=0}^{p-1}$, satisfying $\langle \xi_r, (\sigma-1)^s \rangle = \delta_{r,s}$. Since $\{\pi^{ri_2}\xi_r\}_{r=0}^{p-1}$ is a basis for $\mathcal{H}_{i_2}^*$,

$$a = \sum_{r=0}^{p-1} a_r \xi_r \in \mathcal{H}_{i_2}^* \text{ if and only if } (a_0, a_1, \dots, a_{p-1}) \in R \oplus P^{i_2} \oplus \cdots \oplus P^{(p-1)i_2}.$$

Note that $\epsilon_{\mathcal{H}_{i_2}^*}(a) = 0$ implies $a_0 = 0$. In a similar way, elements

$$b = \sum_{r,s=0}^{p-1} b_{r,s} \xi_r \otimes \xi_s \in \mathcal{H}_{i_2}^* \otimes \mathcal{H}_{i_2}^*$$

can be identified with $p \times p$ matrices $(b_{r,s})_{r,s-0}^{p-1}$ with coefficients satisfying $b_{r,s} \in P^{(r+s)i}$. Furthermore, $(\epsilon_{\mathcal{H}_{i_2}^*} \otimes \epsilon_{\mathcal{H}_{i_2}^*})(b) = 0$ implies that $b_{0,0} = 0$.

We begin by analyzing the elements of $\mathcal{H}_{i_2}^* \otimes \mathcal{H}_{i_2}^*$ that correspond to coboundaries. Suppose $a \in \mathcal{H}_{i_2}^*$ corresponds to a morphism in $\mathrm{Mor}_0(\mathbb{D}_{i_2}^*, \mathbb{G}_a)$. By (1), each $1 \otimes a - \Delta(a) + a \otimes 1 \in \mathcal{H}_{i_2}^* \otimes \mathcal{H}_{i_2}^*$ is identified, via coefficients of $\xi_r \otimes \xi_s$, with the $p \times p$ matrix $(c_{r,s})_{r,s=0}^{p-1}$ where

$$c_{r,s} = \begin{cases} 0 & \text{when } r = 0, s = 0, \text{ or } r + s \geq p, \\ -a_{r+s} & \text{when } 1 \leq r, s, r + s < p. \end{cases}$$

An antidiagonal is a diagonal oriented from lower–left to upper–right. An antidiagonal containing entries with indices r, s where $r + s = k$ is called the kth antidiagonal. We have found that coboundaries correspond to R-valued matrices $(c_{r,s})_{r,s=0}^{p-1}$ with the first column and first row zero and all other entries equal along its antidiagonals. Indeed, the other entries in the kth antidiagonal with $2 \leq k < p$ are equal and lie in P^{ki}. The entries in the kth antidiagonal for $p \leq k \leq 2p-2$ are zero. For example, when $p = 5$ we have

$$(c_{r,s})_{r,s=0}^{4} = -\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & a_2 & a_3 & a_4 & 0 \\ 0 & a_3 & a_4 & 0 & 0 \\ 0 & a_4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Cocycles correspond to elements $\sum_{r,s=0}^{p-1} b_{r,s}\xi_r \otimes \xi_s \in \mathcal{H}_{i_2}^* \otimes \mathcal{H}_{i_2}^*$ that because they lie in the kernel of $\varepsilon_{\mathcal{H}_{i_2}^*} \otimes \varepsilon_{\mathcal{H}_{i_2}^*}$ satisfy $b_{r,0} = b_{0,s} = 0$. They also satisfy $b_{r,s} \in P^{(r+s)i}$, and most importantly (8), which when written out explicitly using (1) becomes

(9)

$$\begin{aligned}0 = \sum_{r,s=1}^{p-1} b_{r,s}\big((\xi_0\otimes\xi_r\otimes\xi_s) - (\Delta(\xi_r)\otimes\xi_s) + (\xi_r\otimes\Delta(\xi_s)) - (\xi_r\otimes\xi_s\otimes\xi_0)\big)\\ = \sum_{r,s=1}^{p-1} b_{r,s}\left(\sum_{c=1}^{s-1}\xi_r\otimes\xi_{s-c}\otimes\xi_c - \sum_{a=1}^{r-1}\xi_a\otimes\xi_{r-a}\otimes\xi_s\right).\end{aligned}$$

Since $\{\xi_u\otimes\xi_v\otimes\xi_w\}_{u,v,w=0}^{p-1}$ is an R-basis for $RC_p^*\otimes RC_p^*\otimes RC_p^*$, the coefficients in this equation must be zero. We will use this fact to characterize the $b_{r,s}$.

First we prove $b_{r,s} = 0$ for $r+s > p$. Observe that $\xi_r\otimes\xi_{p-r}\otimes\xi_{r+s-p}$ appears in (9) with coefficient $b_{r,s}$ for $c = r+s-p$. Furthermore, it appears only once, since for it to appear again with coefficient $-b_{r',s'}$ we would have to have $\xi_r\otimes\xi_{p-r}\otimes\xi_{r+s-p} = \xi_a\otimes\xi_{r'-a}\otimes\xi_{s'}$ for some $1\le r', s'\le p-1$ and $1\le a\le r'-1$. Thus $b_{r,s}=0$.

Next we prove that $b_{r,s} = b_{r',s'}$ for all $r,s,r',s'\ge 1$ such that

$$r+s = r'+s' = k \le p-1.$$

When $k=2$ there is only one coefficient to consider, namely $b_{1,1}$. So assume that $3\le k\le p-1$. Observe that the term $\xi_1\otimes\xi_1\otimes\xi_{k-2}$ appears twice in (9), and thus has coefficient $b_{2,k-2} - b_{1,k-1} = 0$. The term $\xi_2\otimes\xi_1\otimes\xi_{k-3}$ appears twice with coefficient $b_{3,k-3} - b_{2,k-2} = 0$, and so forth until we conclude with the fact that the $\xi_{k-2}\otimes\xi_1\otimes\xi_1$ appears twice, with coefficient $b_{k-1,1} - b_{k-2,2} = 0$. From this the result follows.

In summary, the matrix form $(b_{r,s})$ of a cocycle has entries that satisfy: $b_{r,0} = b_{0,s} = 0$ for $0\le r,s\le p-1$; $b_{r,s} = 0$ for $r+s>p$; and $b_{r,s} = b_{r',s'}\in P^{(r+s)i_2}$ for all $r,s,r',s'\ge 1$ such that $r+s = r'+s'\le p-1$. For an example, take $p=5$. Setting $d_{r+s} = b_{r,s}$ for $1\le r,s$ and $r+s\le p$, we obtain

$$(b_{r,s})_{r,s=0}^{4} = \begin{pmatrix}0&0&0&0&0\\0&d_2&d_3&d_4&d_5\\0&d_3&d_4&d_5&0\\0&d_4&d_5&0&0\\0&d_5&0&0&0\end{pmatrix}.$$

Now from our characterization of the coboundaries above, $\mathrm{H}_0^2(\mathbb{D}_{i_2}^*, \mathbb{G}_a)$ is identified with R-valued matrices $(w_{r,s})_{r,s=0}^{p-1}$ with nontrivial coefficients only on the p-antidiagonal, namely

$$w_{r,s} = \begin{cases} w\in P^{pi_2} & \text{for } r+s=p,\\ 0 & \text{otherwise.}\end{cases}$$

A similar argument shows that $\mathrm{H}_0^2(\mathbb{C}_{p,K}, \mathbb{G}_{a,K})$ can also be identified with K-valued matrices $(\tilde{w}_{r,s})_{r,s=0}^{p-1}$ nontrivial only on the p-antidiagonal, namely those with

$$\tilde{w}_{r,s} = \begin{cases} \tilde{w} \in K & \text{for } r+s=p, \\ 0 & \text{otherwise.} \end{cases}$$

As a result, the map $\mathrm{H}^2_0(\mathbb{D}^*_{i_2}, \mathbb{G}_a) \to \mathrm{H}^2_0(\mathbb{C}_{p,K}, \mathbb{G}_{a,K})$ is an injection. The result follows. □

Corollary 4.4. *There is an isomorphism*

$$\rho : \mathrm{coker}(\Psi_1 : \mathrm{Hom}(\mathbb{D}^*_{i_2}, \mathbb{G}_a)^{\circlearrowleft})_{gt} \to \mathrm{Ext}^1_{gt}(\mathbb{D}^*_{i_2}, \mathbb{D}^*_{i_1}).$$

Proof. This follows from Proposition 4.3 and the top row of diagram (7). □

In order to compute the elements of $\mathrm{Ext}^1_{gt}(\mathbb{D}^*_{i_2}, \mathbb{D}^*_{i_1})$, we need the following.

Proposition 4.5. *The group* $\mathrm{coker}(\Psi_1 : \mathrm{Hom}(\mathbb{D}^*_{i_2}, \mathbb{G}_a)^{\circlearrowleft})_{gt}$ *is isomorphic to the additive subgroup of $K/(\mathbb{F}_p + P^{i_2 - i_1})$ represented by those elements $\mu \in K$ satisfying $\wp(\mu) \in P^{i_2 - pi_1}$.*

Proof. Homomorphisms of R-group schemes correspond to R-Hopf algebra homomorphisms. This means that each element of $\mathrm{Hom}(\mathbb{D}^*_{i_2}, \mathbb{G}_a)$ corresponds to a R-Hopf algebra homomorphism from $R[x]$ to $\mathcal{H}^*_{i_2}$, which since x is primitive, means that this is also a correspondence to $\mathrm{Prim}(\mathcal{H}^*_{i_2})$, the primitive elements in $\mathcal{H}^*_{i_2}$. Applying Proposition 2.2 to $\mathcal{H}^*_{i_2}$, we see that $\mathcal{P} = \mathrm{Prim}(\mathcal{H}^*_{i_2}) = R\beta_2$ where $\beta_2 = \pi^{i_2}\xi_{0,1}$. Notation chosen to be consistent with Proposition 3.2. Define $\mathcal{F} = R\xi_{0,1}$. Note that $\mathcal{P} \subseteq \mathcal{F}$. Similarly, elements of $\mathrm{Hom}(K \otimes_R \mathbb{D}^*_{i_2}, K \otimes_R \mathbb{G}_a)$ correspond to elements of $\mathrm{Prim}(K \otimes_R \mathcal{H}^*_{i_2}) = K\xi_{0,1} = K \otimes_R \mathcal{P}$. Recall from (6), the definition of Ψ_1. Each element in the image of Ψ_1 within $\mathrm{Hom}(\mathbb{D}^*_{i_2}, \mathbb{G}_a)$ corresponds to an element of $\psi(\mathcal{P}) = \psi(R\beta_2)$ within $\mathcal{P} = R\beta_2$. The cokernel is the quotient $\mathcal{P}/\psi(\mathcal{P})$. Except, we are only interested in the generically trivial part, namely those elements of $\mathrm{Hom}(\mathbb{D}^*_{i_2}, \mathbb{G}_a)$ that lie in the image of Ψ_1 from $\mathrm{Hom}(K \otimes_R \mathbb{D}^*_{i_2}, K \otimes_R \mathbb{G}_a)$. These correspond to elements of $(\psi(K \otimes_R \mathcal{F}) \cap \mathcal{P})/\psi(\mathcal{P})$. Elements of $K \otimes_R \mathcal{F}$ can be expressed as $\mu\pi^{i_1}\xi_{0,1}$ for some $\mu \in K$. Since $\xi^p_{0,1} = \xi_{0,1}$, an element of $\psi(K \otimes_R \mathcal{F})$ is expressible as $\wp(\mu)\pi^{pi_1}\xi_{0,1} = \psi(\mu\pi^{i_1}\xi_{0,1})$. It lies in $\mathcal{P}$ precisely when $\wp(\mu) \in P^{i_2 - pi_1}$. It is zero in the quotient $(\psi(K \otimes_R \mathcal{F}) \cap \mathcal{P})/\psi(\mathcal{P})$ precisely when $\mu \in \mathbb{F}_p + P^{i_2 - i_1}$. □

We are now prepared for our classification result.

Theorem 4.6. *Each class $[E] \in \mathrm{Ext}^1_{gt}(\mathbb{D}^*_{i_2}, \mathbb{D}^*_{i_1})$ corresponds to a short exact sequence*

$$E_\mu : \ 0 \to \mathbb{D}^*_{i_1} \longrightarrow \mathrm{Spec}\ R[\pi^{i_1}(\xi_{1,0} - \mu\xi_{0,1}), \pi^{i_2}\xi_{0,1}] \longrightarrow \mathbb{D}^*_{i_2} \to 0$$

where $\mu \in K$ represents a coset in $K/(\mathbb{F}_p + P^{i_2 - i_1})$ that satisfies $\nu_K(\wp(\mu)) \geq i_2 - pi_1$.

Proof. Let $[E] \in \mathrm{Ext}^1_{gt}(\mathbb{D}^*_{i_2}, \mathbb{D}^*_{i_1})$. By Corollary 4.4, $\rho^{-1}([E]) = [h]$ is a class in the cokernel represented by a homomorphism $h : \mathbb{D}^*_{i_2} \to \mathbb{G}_a$. Applying Remark 4.1 to the short exact sequence (6), we conclude that the image of h under connecting homomorphism is the class $[\mathbb{D}^*_h]$ of the pull-back

$$\mathbb{D}^*_h = \{(x, y) \in \mathbb{D}^*_{i_2} \times \mathbb{G}_a : \; h(x) = \Psi_1(y)\}.$$

From the proof of Proposition 4.5, $h : \mathbb{D}^*_{i_2} \to \mathbb{G}_a$ is determined by a Hopf algebra map $\alpha : x \mapsto \wp(-\mu)\pi^{pi_1}\xi_{0,1} = -\wp(\mu)\pi^{pi_1}\xi_{0,1}$ for some $\mu \in K$ with $\nu_K(\wp(\mu)) \geq i_2 - pi_1$. The representing Hopf algebra $\mathcal{H}^*_h$ of $\mathbb{D}^*_h$ arises from the push-out

$$\begin{tikzcd}
\mathcal{H}^*_h & R[x] \arrow[l] \\
\mathcal{H}^*_{i_2} \arrow[u] & R[x] \arrow[l, "\alpha"'] \arrow[u, "\psi"']
\end{tikzcd}$$

where because $\mu\pi^{i_1} \in R$ follows from $\wp(\mu)\pi^{pi_1} \in R$, and $\psi(\mu\pi^{i_1}) = \wp(\mu)\pi^{pi_1}$,

$$\mathcal{H}^*_h = \frac{R[\pi^{i_2}\xi_{0,1}] \otimes_R R[x]}{\wp(\mu)\pi^{pi_1} \otimes 1 + 1 \otimes \psi(x)} \cong \frac{R[\pi^{i_2}\xi_{0,1}][x]}{\psi(x) + \wp(\mu)\pi^{pi_1}\xi_{0,1}} = \frac{R[\pi^{i_2}\xi_{0,1}][x]}{\psi(x + \mu\pi^{i_1}\xi_{0,1})}.$$

Therefore, with $x \mapsto \pi^{i_1}\xi_{1,0}$, under $R[x] \to R[x]/\psi(x) \cong R[\pi^{i_1}\xi_{1,0}]$, one obtains $\mathcal{H}^*_h \cong R[\pi^{i_1}(\xi_{1,0} - \mu\xi_{0,1}), \pi^{i_2}\xi_{0,1}]$, and the result follows. □

5. Parameter Spaces and Endomorphism Rings

The Hopf orders classified in §4 are described in terms of 5 parameters, which provide a 5-tuple in the parameter space. They are (on the group ring side): a choice of two generators σ_1, σ_2 for the group (a $\mathbb{F}_p$-basis for the vector space $\langle \sigma_1, \sigma_2 \rangle$), two nonnegative integers i_1, i_2 (whose sum determines the discriminant of $\mathcal{H}^*$, also the index $[\mathcal{H} : RC_p^2]$), and an element $\mu \in K$ that satisfies $\nu_K(\wp(\mu)) \geq i_2 - pi_1$ and may be chosen to satisfy Convention 1, so that $\mu \in K$ is an element of largest valuation in $\mu + \mathbb{F}_p + P^{i_2 - i_1}$.

5.1. Navigating the parameter space.

We are interested in navigating this parameter space by determining all alternative parameters (group generators σ_1', σ_2', nonnegative integers i_1', i_2' and elements $\mu' \in K$ that satisfy $i_2' - pi_1' \leq \nu_K(\wp(\mu'))$ and Convention 1) that describe the same Hopf order:

$$\mathcal{H} = R\left[\frac{\sigma_1 - 1}{\pi^{i_1}}, \frac{\sigma_2\sigma_1^{[\mu]} - 1}{\pi^{i_2}}\right] = R\left[\frac{\sigma_1' - 1}{\pi^{i_1'}}, \frac{\sigma_2'(\sigma_1')^{[\mu']} - 1}{\pi^{i_2'}}\right] = \mathcal{H}'. \tag{10}$$

We consider the more interesting case when $\mu \neq 0$ first.

Proposition 5.1. *Let $\mathcal{H}$ be a Hopf order in KC_p^2 satisfying Convention 1 and $\mu \neq 0$, so that $\nu_K(\mu) < i_2 - i_1$. Let $m = \nu_K(\mu)$, then $\nu_K(\wp(\mu)) = \min\{m, pm\}$. Given a matrix*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p),$$

define $\mathcal{H}^A = \mathcal{H}'$ by setting $(\sigma_1', \sigma_2') = (\sigma_1^a\sigma_2^c, \sigma_1^b\sigma_2^d)$, which can be expressed as $(\sigma_1', \sigma_2') = (\sigma_1, \sigma_2)\cdot A$; by, using a linear fractional transformation, setting

$$\mu' = A^{-1}(\mu) = \frac{d\mu - b}{a - c\mu};$$

and finally, by setting

$$(i_1', i_2') = \begin{cases} (i_1 + m, i_2 - m) & \text{if } \nu_K(a - c\mu) = m \neq 0, \\ (i_1, i_2) & \text{otherwise.} \end{cases}$$

Then $\mathcal{H}^A = \mathcal{H}$. Conversely, assume $\mathcal{H}' = \mathcal{H}$ with $\mu' \neq 0$ satisfying Convention 1, then there is a matrix $A \in \mathrm{GL}_2(\mathbb{F}_p)$ such that $\mathcal{H}' = \mathcal{H}^A$.

Proof. To show that $\mathcal{H}^A$ is a Hopf order, it is enough to show that $\mu' = A^{-1}(\mu)$ and (i_1', i_2') satisfy two inequalities:

$$i_2' - pi_1' \leq \nu_K(\wp(\mu')) \quad \text{and} \quad \nu_K(\mu') < i_2' - i_1',$$

since clearly σ_1', σ_2' generate the group. We consider cases: If $\nu_K(\mu) = m = 0$, it is easy to see that Convention 1 implies $\nu_K(\mu') = 0$ and the desired inequalities hold. If $\nu_K(\mu) = m \neq 0$ observe that $\nu_K(a - c\mu) = m$ if and only if $a = 0, m > 0$, or $c \neq 0, m < 0$.

If $\nu_K(\mu) = m > 0$ then

$$\mu' = \begin{cases} -d/c + b\mu^{-1}/c & \text{for } a = 0, \\ (1/a)(-b + \det(A)\mu/a) \bmod \mu^2 R & \text{for } a \neq 0. \end{cases}$$

Observe that $a = 0$ implies $c \neq 0$. In any case, when $a \neq 0$, $(i_1', i_2') = (i_1, i_2)$ and $\nu_K(\wp(\mu')) = \nu_K(\wp(\mu))$ and $\nu_K(\mu') \leq \nu_K(\mu)$. Thus the two inequalities hold. The situation when $a = 0$ is more interesting. In this case,

$$(i_1', i_2') = (i_1 + m, i_2 - m), \quad \nu_K(\wp(\mu')) = -pm \quad \text{and} \quad \nu_K(\wp(\mu)) = m.$$

Observe that $m \geq i_2 - pi_1$ is equivalent to

$$-pm \geq i_2' - pi_1' = (i_2 - m) - p(i_1 + m).$$

Additionally, since $m < i_2 - i_1$, $\nu_K(\mu') = -m < i_2' - i_1'$.

If $\nu_K(\mu) = m < 0$ then

$$\mu' = \begin{cases} -b/a + d\mu/a & \text{for } c = 0, \\ (-1/c)(d + \det(A)\mu^{-1}/c) \bmod \mu^{-2} R & \text{for } c \neq 0. \end{cases}$$

Again, $c = 0$ implies $a \neq 0$. If $c = 0$, it is easy to see that the two inequalities hold. The interesting inequality occurs when $c \neq 0$. In this case, $\nu_K(\wp(\mu')) = -m$ and $\nu_K(\wp(\mu)) = pm$ with $pm \geq i_2 - pi_1$ equivalent to $-m \geq i_2' - pi_1' = (i_2 - m) - p(i_1 + m)$. Similarly, $\nu_K(\mu') < i_2' - i_1'$. At this point we have established that $\mathcal{H}^A$ is a Hopf order.

Two Hopf orders $\mathcal{H}, \mathcal{H}'$ are equal if and only if their duals are equal $(\mathcal{H}')^* = \mathcal{H}^*$. If their duals are equal, the discriminants of their duals are equal $\mathrm{disc}((\mathcal{H}')^*) = \mathrm{disc}(\mathcal{H}^*)$. Using Proposition 3.2, leads to the requirement that $i_1' + i_2' = i_1 + i_2$. Two dual Hopf orders with the same discriminants are the same if and only if one is contained in the other, namely $\mathcal{H}^* = R[\beta_1, \beta_2] \subseteq (\mathcal{H}')^*$. As in the proof of Theorem 3.6, we define $\alpha'_{r,s} = (\sigma_1' - 1)^r(\sigma_2'(\sigma_1')^{[\mu']} - 1)^s/\pi^{ri_1'+si_2'}$. Again, we let $\sigma_1 = 1 + x$ and $\sigma_2 = 1 + y$, and observe that $\xi_{1,0}$ and $\xi_{0,1}$ both act trivially on elements of $(x, y)^2$. Furthermore, $(\sigma_1' - 1) \equiv ax + cy \pmod{(x, y)^2}$ and $(\sigma_2'(\sigma_1')^{[\mu]}-1) \equiv (b+a\mu')x+(d+c\mu')y \pmod{(x, y)^2}$. As a result, the requirement that $\langle\beta_1, \alpha'_{r,s}\rangle \in R$ is equivalent to two conditions: $a - c\mu \in P^{i_1'-i_1}$, and $b + a\mu' - d\mu - c\mu\mu' \in P^{i_2'-i_1}$; while $\langle\beta_2, \alpha'_{r,s}\rangle \in R$ becomes two further conditions: $c \in P^{i_1'-i_2}$ and $d + c\mu' \in P^{i_2'-i_2}$. This leads to the following necessary and sufficient conditions for $\mathcal{H} = \mathcal{H}'$: First, $i_1' + i_2' = i_1 + i_2$ and second,

$$c \in P^{i_1'-i_2}, \tag{11}$$

$$a - c\mu \in P^{i_1'-i_1}, \tag{12}$$

$$d + c\mu' \in P^{i_2'-i_2}, \tag{13}$$

$$b + a\mu' - d\mu - c\mu\mu' \in P^{i_2'-i_1}. \tag{14}$$

We could prove that $\mathcal{H}^A = \mathcal{H}$ by using the well-known decomposition of $A \in \mathrm{GL}_2(\mathbb{F}_p)$ into a product of elementary matrices, namely matrices of the form

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \text{ with } b \in \mathbb{F}_p, \quad \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \text{ with } a \in \mathbb{F}_p^\times, \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

applying the elementary matrices in succession. We leave this approach to the reader, and apply the matrix $A \in \mathrm{GL}_2(\mathbb{F}_p)$ in one step. Observe that the definition of μ' means that $b + a\mu' - d\mu - c\mu\mu' = 0$. One consequence is that (14) holds vacuously. Another is $-\det(A) + (a - c\mu)(d + c\mu') = 0$, which means that

$$\nu_K(a - c\mu) + \nu_K(d - c\mu') = 0. \tag{15}$$

We are concerned with verifying (11) through (13). There are two cases: Either $\nu_K(a - c\mu) = 0$ or $\nu_K(a - c\mu) = m$. If $\nu_K(a - c\mu) = 0$, then using (15), $\nu_K(d - c\mu') = 0$. Because $(i_1', i_2') = (i_1, i_2)$, (12) and (13) hold, and (11) follows, since $\nu_K(\mu) = m < i_2 - i_1$ implies $\mathbb{F}_p \subset P^{i_1'-i_2}$. This leaves $\nu_K(a - c\mu) = m$. Using (15), $\nu_K(d - c\mu') = -m$. Because $(i_1', i_2') = (i_1 + m, i_2 - m)$, (12) and (13) hold immediately. Furthermore, because $i_1 + m - i_2 < 0$, (11) holds. We have proven $\mathcal{H}^A = \mathcal{H}$.

Assume for the converse that $\mathcal{H}' = \mathcal{H}$ with both $\mu, \mu' \neq 0$, and both μ, μ' satisfying Convention 1. Observe that by applying the elementary matrix

$$B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{16}$$

to one or both of $\mathcal{H}$ and $\mathcal{H}'$, if one or both of $\nu_K(\mu)$ and $\nu_K(\mu')$ is negative, and then by replacing $\mathcal{H}^B = \mathcal{H}$ or $(\mathcal{H}')^B = \mathcal{H}'$, we may assume, based upon the preceding argument, that $\mathcal{H}$ and $\mathcal{H}'$, without loss of generality, are constructed with $\mu, \mu' \neq 0$ satisfying Convention 1 and $\nu_K(\mu), \nu_K(\mu') \geq 0$. There is necessarily a matrix $A \in \mathrm{GL}_2(\mathbb{F}_p)$ such that $(\sigma_1', \sigma_2') = (\sigma_1^a\sigma_2^c, \sigma_1^b\sigma_2^d)$. Our objective therefore is to show that $\mu' \equiv A^{-1}(\mu) \bmod P^{i_2'-i_1'}$ where (i_1', i_2') is determined from (i_1, i_2) as in the statement of this proposition. Since $\mathcal{H}' = \mathcal{H}$ we know that $i_1' + i_2' = i_1 + i_2$ and also that (11) through (14) hold. Since (14) is equivalent to $\mu' \equiv A^{-1}(\mu) \bmod P^{i_2'-i_1}$, it is enough to prove $(i_1', i_2') = (i_1, i_2)$. Observe that $\nu_K(a - c\mu), \nu_K(d + c\mu') \geq 0$.

Case 1. If $\nu_K(a - c\mu) = \nu_K(d + c\mu') = 0$, then (12) implies $i_1 \geq i_1'$ and (13) implies $i_2 \geq i_2'$. Using $i_1' + i_2' = i_1 + i_2$, this means that $(i_1', i_2') = (i_1, i_2)$.

Case 2. Assume $\nu_K((a - c\mu)(d + c\mu')) > 0$. This means that $c \neq 0$, because if $c = 0$ then, using $\det(A) \neq 0$, $ad \neq 0$, which would mean that

$$\nu_K(a - c\mu) = \nu_K(d + c\mu') = 0.$$

Since $c \neq 0$, (11) implies $i_2 \geq i_1'$ and (14) is equivalent to

$$-\det(A) + (a - c\mu)(d + c\mu') \in P^{i_2'-i_1},$$

which using $\nu_K((a - c\mu)(d + c\mu')) > 0$ implies $i_1 \geq i_2'$. Using $i_1' + i_2' = i_1 + i_2$, $(i_1', i_2') = (i_2, i_1)$. □

We now consider the case $\mu = 0$.

Proposition 5.2. *Let $\mathcal{H}$ be a Hopf order in KC_p^2 satisfying $\mu = 0$. Given*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p),$$

define $\mathcal{H}^A = \mathcal{H}'$ with $\mathcal{H}'$ as in (10) by setting $(\sigma_1', \sigma_2') = (\sigma_1^a\sigma_2^c, \sigma_1^b\sigma_2^d)$, setting

$$\mu' = \begin{cases} 0 & \text{if } i_1 = i_2, \text{ or } a = 0, i_2 > i_1, \text{ or } c = 0, i_2 < i_1, \\ -b/a & \text{if } a \neq 0, i_2 > i_1, \\ -d/c & \text{if } c \neq 0, i_2 < i_1, \end{cases}$$

and by setting

$$(i_1', i_2') = \begin{cases} (i_1, i_2) & \text{if } i_2 = i_1, \text{ or } a \neq 0, i_2 > i_1, \text{ or } c = 0, i_2 < i_1, \\ (i_2, i_1) & \text{if } a = 0, i_2 > i_1, \text{ or } c \neq 0, i_2 < i_1. \end{cases}$$

Then $\mathcal{H}^A = \mathcal{H}$. Conversely, assume $\mathcal{H}' = \mathcal{H}$, then there is a matrix $A \in \mathrm{GL}_2(\mathbb{F}_p)$ such that $\mathcal{H}' = \mathcal{H}^A$.

Proof. We leave it to the reader to verify that under the stated conditions $\mathcal{H}^A = \mathcal{H}$. This can be seen by direct algebraic manipulations, or by using (11) through (14). We focus on the converse. To begin observe if $i_1 \neq i_2$, four possible outcomes are listed: $i_2 < i_1, c = 0$; $i_2 < i_1, c \neq 0$; $i_2 > i_1, a \neq 0$; and $i_2 > i_1, a = 0$. There are four cases. To avoid repeating the same argument four times, we begin by observing that because $\mu = 0$ we can (by relabeling the presentation of $\mathcal{H}$ if necessary) assume that without loss of generality $i_2 \le i_1$. Thereby we reduce the number of these cases to two.

Assume now that $\mathcal{H} = \mathcal{H}'$ where $\mathcal{H}'$ is as in (10). There is necessarily a matrix $A \in \mathrm{GL}_2(\mathbb{F}_p)$ such that $(\sigma_1', \sigma_2') = (\sigma_1^a\sigma_2^c, \sigma_1^b\sigma_2^d)$. While we don't assume that $\mu' = 0$, we may assume that μ' satisfies Convention 1. By doing so, note that we may have had to replace the matrix A with another matrix A' in $\mathrm{GL}_2(\mathbb{F}_p)$. Our goal now is to prove $\mathcal{H}' = \mathcal{H}^{A'}$. We expect to find that $\mu' = 0$. However to avoid introducing too much notation (e.g., $a', b', c', d' \in \mathbb{F}_p$), we simply use the entries of A to refer to the entries of A'.

As in the proof of Proposition 5.1, the discriminants of the duals of these Hopf orders are the same. Thus $i_1' + i_2' = i_1 + i_2$. Furthermore, (11) through (14) must be satisfied from which we find that $c \in P^{i_1'-i_2}$, $a \in P^{i_1'-i_1}$, $d + c\mu' \in P^{i_2'-i_2}$, and $b + a\mu' \in P^{i_2'-i_1}$. Because of Convention 1,

$$v_K(d + c\mu') = \min\{v_K(d), v_K(c\mu')\},$$
$$v_K(b + a\mu') = \min\{v_K(b), v_K(a\mu')\}.$$

Thus we have the following necessary and sufficient conditions for $\mathcal{H} = \mathcal{H}'$:

$$\begin{aligned} &a \in P^{i_1'-i_1}, \quad c \in P^{i_1'-i_2}, \quad c\mu' \in P^{i_2'-i_2},\\ &d \in P^{i_2'-i_2}, \quad b \in P^{i_2'-i_1}, \quad a\mu' \in P^{i_2'-i_1}, \end{aligned} \tag{17}$$

and $i_1' + i_2' = i_1 + i_2$. We also know that $\det(A') = ad - bc \neq 0$.

Suppose that all of a, b, c, d are nonzero. Then $a \in P^{i_1'-i_1}$ implies $i_1' \le i_1$. Similarly $i_2' \le i_2$, $i_1' \le i_2$, and $i_2' \le i_1$ follow from (17). Because $i_1' + i_2' = i_1 + i_2$, $i_1' = i_1 = i_2' = i_2$. Thus $v_K(c\mu') \ge i_2' - i_1'$, which, since μ' satisfies Convention 1, means that $\mu' = 0$.

If $ad = 0$, then because $\det(A') \neq 0$, $bc \neq 0$. Since $b \neq 0$ and $c \neq 0$, $i_1' \le i_2$ and $i_2' \le i_1$ follow from (17). Using $i_1' + i_2' = i_1 + i_2$, $i_1' = i_2$ and $i_2' = i_1$. Since $v_K(c\mu') \ge i_2' - i_2 = i_2' - i_1'$, by Convention 1, $\mu' = 0$. Similarly, if $bc = 0$, then $ad \neq 0$ and from (17), we see that $i_1' \le i_1$ and $i_2' \le i_2$. Using $i_1' + i_2' = i_1 + i_2$, $i_1' = i_1$ and $i_2' = i_2$. So $v_K(a\mu') \ge i_2' - i_1 = i_2' - i_1'$, and thus $\mu' = 0$. In all cases, $\mu' = 0$.

Now that we know $\mu' = 0$, we can reduce the need to treat the remaining two cases to one by assuming, without loss of generality, that $\mathcal{H}'$ has been presented with $i_2' \le i_1'$. Since doing so may involve relabeling $\mathcal{H}'$, including a switch in the columns of A' resulting in $A'' \in \mathrm{GL}_2(\mathbb{F}_p)$, we now begin again at the top of this argument, using the entries of A to refer to entries of A''. Beginning with (17), the situation where $abcd \neq 0$ is just as before, and there is no further condition on A''. So we consider now the two cases $ad = 0$ and $bc = 0$ in greater detail. If $ad = 0$, then as we saw earlier, $i_1' = i_2$ and $i_2' = i_1$. Since we have assumed $i_2 \le i_1$ and $i_2' \le i_1'$, we find $i_1' = i_1 = i_2' = i_2$ and (17) holds without further restriction on $A'' \in \mathrm{GL}_2(\mathbb{F}_p)$. Suppose $bc = 0$. Then as we saw earlier, $i_1' = i_1$ and $i_2' = i_2$. If $c \neq 0$, then from (17), $i_1' \le i_2$

or $i_1 \leq i_2$. Thus, since by assumption $i_2 \leq i_1$, we have $i_1 = i_2$. On the other hand, if $b \neq 0$, then $c = 0$ and $i_2' \leq i_1$, which becomes $i_2 \leq i_1$. As a result, $\mathcal{H}' = \mathcal{H}^{A''}$. □

5.2. Endomorphism ring of a Hopf order. A Hopf algebra endomorphism φ of one of the Hopf orders $\mathcal{H}$ in KC_p^2, as classified in Theorem 4.6, is an R-module endomorphism that respects the coalgebraic properties and antipode, as well as the algebraic properties of $\mathcal{H}$. As a result, φ fixes the field K, and maps grouplike elements to grouplike elements, which means that it can be identified as φ_M for some

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{F}_p),$$

where $\varphi_M(\sigma_1) = \sigma_1^M = \sigma_1^a\sigma_2^c$, $\varphi_M(\sigma_2) = \sigma_2^M = \sigma_1^b\sigma_2^d$, and furthermore that

$$\varphi_M\mathcal{H} = R\left[\frac{\sigma_1^M - 1}{\pi^{i_1}}, \frac{\sigma_2^M(\sigma_1^M)^{[\mu]} - 1}{\pi^{i_2}}\right] \subseteq \mathcal{H} = R\left[\frac{\sigma_1 - 1}{\pi^{i_1}}, \frac{\sigma_2(\sigma_1)^{[\mu]} - 1}{\pi^{i_2}}\right],$$

where $\mu \in K$ satisfies $\nu_K(\wp(\mu)) \geq i_2 - pi_1$ and $i_1, i_2 \geq 0$. Since $\mathcal{H}$ is an abelian Hopf algebra (commutative and cocommutative), the set of all such endomorphisms of $\mathcal{H}$, which we denote by $\mathrm{End}(\mathcal{H})$, is a ring under convolution and composition [Chi00, Prop 1.10]. Given $M, N \in M_2(\mathbb{F}_p)$, one sees that $\varphi_M * \varphi_N = \varphi_{M+N}$ and $\varphi_M \circ \varphi_N = \varphi_{MN}$, and so $\mathrm{End}(\mathcal{H})$ can be identified with a subring of $M_2(\mathbb{F}_p)$, which can furthermore be classified by isomorphism type. The result, as displayed below, is that $\mathrm{End}(\mathcal{H})$ is isomorphic to one of four rings: $\mathbb{F}_p$, $\mathbb{F}_{p^2}$, the ring of all upper triangular matrices $\mathbb{T} \subset M_2(\mathbb{F}_p)$, and $M_2(\mathbb{F}_p)$ itself.

Proposition 5.3. *Given a Hopf order $\mathcal{H}$ in KC_p^2 with parameters $i_1, i_2 \geq 0$, $\sigma_1, \sigma_2 \in C_p^2$, $\mu \in K$ such that $\nu_K(\mu) \geq i_2 - pi_1$ satisfying Convention 1. Then*

$$\mathrm{End}(\mathcal{H}) \cong \begin{cases} M_2(\mathbb{F}_p) & \mu = 0, i_1 = i_2, \\ \mathbb{T} & \mu = 0, i_1 \neq i_2, \\ \mathbb{F}_{p^2} & \mu \neq 0, \mu \in \mathbb{F}_{p^2}, \\ \mathbb{F}_p & \mu \neq 0, \mu \notin \mathbb{F}_{p^2}. \end{cases}$$

Remark 5.4. The Hopf orders with $\mathrm{End}(\mathcal{H}) \cong \mathbb{F}_{p^2}$ were studied by Raynaud [Ray74]. They necessarily satisfy $\mu \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ and $i_2 > i_1$.

Proof. Given $\mathcal{H}$. Without loss of generality we may assume $\mu \in R$, for if $\nu_K(\mu) < 0$, we can use Proposition 5.1 and apply B, as defined in (16). This application of B preserves the Hopf order, but changes the parameters, which we relabel so that μ' is expressed as μ. The new μ satisfies Convention 1 for the new i_1, i_2. Observe furthermore that B does not change whether $\mu \in \mathbb{F}_{p^2}$ or not.

At this point, $\mu \in R$. Later, we will find it convenient to have expressed $\mu = \mu_0 + \mu_1$ for some $\mu_0 \in k = R/P$ and $\mu_1 \in P$. Observe that if $\mu_0 \in \mathbb{F}_p^\times$, then μ does not satisfy Convention 1. So $\mu_0 = 0$ or $\mu_0 \in k \setminus \mathbb{F}_p$. If $\mu_0 = 0$, then either $\mu_1 = \mu = 0$ or $\nu_K(\mu_1) = \nu_K(\mu) < i_2 - i_1$. If $\mu_0 \in k \setminus \mathbb{F}_p$, then replacing μ_1 by another element of $\mu_1 + P^{i_2-i_1}$ does not change the valuation of μ, nor does it alter the Hopf order. Thus we may assume that either $\mu_1 = 0$ or $\nu_K(\mu_1) < i_2 - i_1$. In any case, μ continues to satisfy Convention 1.

The statement $\varphi_M \mathcal{H} \subseteq \mathcal{H}$ is equivalent to $\langle \mathcal{H}^*, \varphi_M \mathcal{H} \rangle \subseteq R$. Setting $\sigma_1' = \sigma_1^M$, $\sigma_2' = \sigma_2^M$, $\mu' = \mu$, $i_1' = i_1$ and $i_2' = i_2$ so that we can use material from the proof of Proposition 5.1, we see that the statement $\langle \mathcal{H}^*, \varphi_M \mathcal{H} \rangle \subseteq R$ is equivalent to Conditions (11)–(14). Note that since $\mu \in R$, (12), (13) hold without further restriction, and thus the necessary and sufficient conditions for $\varphi_M \in \mathrm{End}(\mathcal{H})$ are

$$c \in P^{i_1-i_2}, \tag{18}$$

$$b + (a-d)\mu - c\mu^2 \in P^{i_2-i_1}. \tag{19}$$

We consider the cases $\mu = 0$ and $\mu \neq 0$ separately.

Assume $\mu = 0$. Then $\varphi_M \in \mathrm{End}(\mathcal{H})$ if and only if $c \in P^{i_1-i_2}$ and $b \in P^{i_2-i_1}$. When $i_2 = i_1$, this restriction is vacuous and $\varphi_M \in \mathrm{End}(\mathcal{H})$ for all $M \in M_2(\mathbb{F}_p)$. When $i_2 > i_1$, $b = 0$ and $\varphi_M \in \mathrm{End}(\mathcal{H})$ for all lower triangular matrices M in $M_2(\mathbb{F}_p)$, while when $i_2 < i_1$, $c = 0$ and $\varphi_M \in \mathrm{End}(\mathcal{H})$ for all $M \in \mathbb{T} \subset M_2(\mathbb{F}_p)$. The two rings of triangular matrices are isomorphic under conjugation by B.

Assume $\mu \neq 0$. There are two basic cases: Either $\mu \notin \mathbb{F}_{p^2}$, or $\mu \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$. In either case, since $\mu \in R$, under Convention 1, $0 \leq \nu_K(\mu) < i_2 - i_1$ and (18) holds vacuously. Replace μ in (19) with $\mu_0 + \mu_1$, and notice that (19) is now equivalent to

$$b + (a-d)\mu_0 - c\mu_0^2 = 0, \tag{20}$$

$$(a-d)\mu_1 - c(2\mu_0\mu_1 + \mu_1^2) \in P^{i_2-i_1}. \tag{21}$$

Meanwhile, the first basic case can be broken in two: Either $\mu_0 \notin \mathbb{F}_{p^2}$, or $\mu_0 \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ with $\mu_1 \neq 0$. Suppose $\mu_0 \notin \mathbb{F}_{p^2}$. Then (20) implies $b = a - d = c = 0$, (21) holds vacuously, and $\varphi_M \in \mathrm{End}(\mathcal{H})$ precisely for $M \in \mathbb{F}_p \cdot I \subset M_2(\mathbb{F}_p)$ where I denotes the identity matrix. Now suppose $\mu_0 \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ with $\mu_1 \neq 0$. Since $0 < \nu_K(\mu_1) < \min\{\nu_K(\mu_1^2), i_2 - i_1\}$, the coefficient of μ_1 in (21) is zero, namely $a - d - 2c\mu_0 = 0$. Since $\mu_0 \notin \mathbb{F}_p$, this means that $c = a - d = 0$, and thus because of (20), $b = 0$ as well. Again, $\varphi_M \in \mathrm{End}(\mathcal{H})$ precisely for $M \in \mathbb{F}_p \cdot I$.

We now consider the second basic case where $\mu \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$. This means that μ satisfies a monic irreducible equation, which we express as

$$f(x) = r + sx + x^2 \in \mathbb{F}_p[x].$$

Since $\mu_0 \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ and $\mu_1 = 0$, (20) and (21) are equivalent to

$$b + (a-d)\mu - c\mu^2 = 0,$$

a statement that is equivalent to $M = aI - cD$ where I is the identity matrix and

$$D = \begin{pmatrix} 0 & r \\ -1 & -s \end{pmatrix}.$$

As a result, $\varphi_M \in \mathrm{End}(\mathcal{H})$ occurs exactly when M lies in the $\mathbb{F}_p$-span of I and D, a vector space that, because D is a root of $f(x)$, is isomorphic to $\mathbb{F}_{p^2}$. □

6. Conclusion

The results of this paper yield the following observation.

Corollary 6.1. *Fixing the two generators σ_1, σ_2 for the group C_p^2, a bijection exists between the Hopf orders $\mathcal{H}$ in KC_p^2 and the set of triples*

$$(i_1, i_2, \mu + P^{i_2-i_1})$$

of two integers $i_1, i_2 \geq 0$ and one coset $\mu + P^{i_2-i_1}$ that satisfies

$$v_K(\wp(\mu)) \geq i_2 - pi_1.$$

This bijection identifies a triple with the presentation

$$R\left[\frac{\sigma_1 - 1}{\pi^{i_1}}, \frac{\sigma_2\sigma_1^{[\mu]} - 1}{\pi^{i_2}}\right].$$

Proof. Proposition 3.4 states that there is a map, via the presentation above, from triples to Hopf orders. Based upon Theorems 4.6 and 3.6, this map is surjective. To address injectivity, observe that if we are given two triples and thus two presentations $\mathcal{H}$ and $\mathcal{H}'$ that used the same fixed generators of the group (so $\sigma_1' = \sigma_1$ and $\sigma_2' = \sigma_2$), and furthermore produce the same Hopf order (thus $\mathcal{H} = \mathcal{H}'$), then we may fully evoke Convention 1 for μ' when we use Propositions 5.1 and 5.2. However we need to recognize that by doing so, we may have had to replace μ' by another element in $\mu' + \mathbb{F}_p$, which requires a change the generators for the group. By returning to the same fixed generators, we conclude that the matrix A is the identity matrix, $(i_1', i_2') = (i_1, i_2)$, and $\mu' \in \mu + P^{i_2-i_1}$. □

References

[Bon00] Bondarko, M. V. Local Leopoldt's problem for rings of integers in abelian p-extensions of complete discrete valuation fields. *Doc. Math.* **5** (2000), 657–693 (electronic). MR1808921, Zbl 0964.11053.

[By93] Byott, N. P. Cleft extensions of Hopf algebras. II. *Proc. London Math. Soc.* (3) **67** (1993), no. 2, 277–304. MR1226603, Zbl 0795.16026, doi: 10.1112/plms/s3-67.2.277.

[ByE05] Byott, Nigel P.; Elder, G. Griffith. New ramification breaks and additive Galois structure. *J. Théor. Nombres Bordeaux* **17** (2005), no. 1, 87–107. MR2152213 (2006b:11149), Zbl 1162.11394, doi: 10.5802/jtnb.479.

[ByE14] Byott, Nigel P.; Elder, G. Griffith. Sufficient conditions for large Galois scaffolds. Preprint, April 2014. arXiv:1308.2092v2.

[Chi00] Childs, Lindsay N. Taming wild extensions: Hopf algebras and local Galois module theory. Mathematical Surveys and Monographs, 80. *American Mathematical Society, Providence, RI*, 2000. viii+215 pp. ISBN: 0-8218-2131-8. MR1767499 (2001e:11116), Zbl 0944.11038, doi: 10.1090/surv/080.

[DG70] Demazure, Michel; Gabriel, Pierre. Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs. *Masson & Cie, Éditeur, Paris; North-Holland Publishing Co., Amsterdam*, 1970. xxvi+700 pp. MR0302656, Zbl 0203.23401.

[Gre92] Greither, C. Extensions of finite group schemes, and Hopf Galois theory over a complete discrete valuation ring. *Math. Z.* **210** (1992), no. 1, 37–67. MR1161169 (93f:14024), Zbl 0737.11038, doi: 10.1007/BF02571782.

[HS71] Hilton, Peter John; Stammbach, Urs. A course in homological algebra. Graduate Texts in Mathematics, 4. *Springer-Verlag, New York-Berlin*, 1971. ix+338 pp. MR0346025, Zbl 0238.18006, doi: 10.1007/978-1-4684-9936-0.

[Koc16] Koch, Alan. Primitively generated Hopf orders in characteristic p. Preprint, to appear in *Comm. Algebra*, 2016. arXiv:1509.07393, doi: 10.1080/00927872.2016.1233235.

[Lan02] Lang, Serge. Algebra. Revised third edition. Graduate Texts in Mathematics, 211. *Springer-Verlag, New York*, 2002. xvi+914 pp. ISBN: 0-387-95385-X. MR1878556, Zbl 0984.00001, doi: 10.1007/978-1-4613-0041-0.

[Mil80] Milne, James S. Étale cohomology. Princeton Mathematical Series, 33. *Princeton University Press, Princeton, N.J.*, 1980. xiii+323 pp. ISBN: 0-691-08238-3. MR559531, Zbl 0433.14012.

[Oor66] Oort, F. Commutative group schemes. Lecture Notes in Mathematics, 15. *Springer-Verlag, Berlin-New York*, 1966. vi+133 pp. MR0213365, Zbl 0216.05603, doi: 10.1007/BFb0097479.

[Ray74] Raynaud, Michel. Schémas en groupes de type $(p, \ldots, p)$. *Bull. Soc. Math. France* **102** (1974), 241–280. MR0419467 (54 #7488), Zbl 0325.14020.

[TO70] Tate, John; Oort, Frans. Group schemes of prime order. *Ann. Sci. École Norm. Sup.* (4) **3** (1970), 1–21. MR0265368 (42 #278), Zbl 0225.14024.

[Tos10] Tossici, Dajano. Models of $\mu_{p^2,K}$ over a discrete valuation ring. *J. Algebra* **323** (2010), no. 7, 1908–1957. MR2594655 (2011c:14127), Zbl 1193.14059, arXiv:1001.1416, doi: 10.1016/j.jalgebra.2010.01.012.

[Und94] Underwood, Robert G. R-Hopf algebra orders in KC_{p^2}. *J. Algebra* **169** (1994), no. 2, 418–440. MR1297158, Zbl 0820.16036, doi: 10.1006/jabr.1994.1293.

[Wat79] Waterhouse, William C. Introduction to affine group schemes. Graduate Texts in Mathematics, 66. *Springer-Verlag, New York-Berlin*, 1979. xi+164 pp. ISBN: 0-387-90421-2. MR547117 (82e:14003), Zbl 0442.14017, doi: 10.1007/978-1-4612-6217-6.

(G. Griffith Elder) Department of Mathematics, University of Nebraska at Omaha, Omaha, Nebraska, U.S.A.
elder@unomaha.edu

(Robert G. Underwood) Department of Mathematics and Computer Science, Auburn University at Montgomery, Montgomery, Alabama, U.S.A
runderwo@aum.edu

This paper is available via http://nyjm.albany.edu/j/2017/23-2.html.