EXTENSIONS OF GROUP SCHEMES IN CHARACTERISTIC p

Robert G. Underwood
Department of Mathematics/Informatics
Auburn University Montgomery
P. O. Box 244023
Montgomery, AL 36124-4023
runderwo@aum.edu

June 30, 2013

1. Introduction

Let p be a prime number, let n be an integer, $n \geq 1$, and let $\mathbb{F}_q$ denote the Galois field with $q = p^n$ elements. Let t be an indeterminate, let $R = \mathbb{F}_q[[t]]$ and let $K = \mathrm{Frac}(R) = \mathbb{F}_q((t))$. R is a local ring with maximal ideal (t); an element $x \in K$ can be written as $x = ut^i$ for some unit $u \in R$, and some $i \in \mathbb{Z}$. The (t)-order of x is $\mathrm{ord}(x) = i$.

Let $C_p \times C_p$ denote the elementary abelian group of order p^2 with σ, τ generating the left and right copies of C_p. Let $C_p \times C_p \to C_p$ denote the canonical surjection defined by $\sigma \mapsto 1$. For integers $i, j \geq 0$, there are Hopf (Larson) orders in KC_p given as

$$H(i) = R\left[\frac{\sigma - 1}{t^i}\right], \quad H(j) = R\left[\frac{\tau - 1}{t^j}\right].$$

Suppose $\mu \in K$ is so that $\mathrm{ord}(\mu) \geq -i + (j/p)$. Then there is an R-Hopf order in $K(C_p \times C_p)$ of the form

$$H(i, j, \mu) = R\left[\frac{\sigma - 1}{t^i}, \frac{\sigma^{[-\mu]}\tau - 1}{t^j}\right],$$

with

$$\sigma^{[-\mu]} = \sum_{m=0}^{p-1} \binom{-\mu}{m} (\sigma - 1)^m,$$

called an Elder order in $K(C_p \times C_p)$ [2].

The Elder order $H(i, j, \mu)$ induces a short exact sequence of R-Hopf orders

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

or equivalently, a short exact sequence of R-group schemes

$$0 \to \operatorname{Spec} H(j) \to \operatorname{Spec} H(i,j,\mu) \to \operatorname{Spec} H(i) \to 0. \tag{1}$$

Sequence (1) represents an equivalence class in $\operatorname{Ext}^1(\operatorname{Spec} H(i), \operatorname{Spec} H(j))$, the group of 1-extensions of $\operatorname{Spec} H(j)$ by $\operatorname{Spec} H(i)$. Over K elements of $\operatorname{Ext}^1(\operatorname{Spec} H(i), \operatorname{Spec} H(j))$ appear as

$$0 \to \boldsymbol{\mu}_{\boldsymbol{p},K} \to \boldsymbol{\mu}_{\boldsymbol{p},K} \times \boldsymbol{\mu}_{\boldsymbol{p},K} \to \boldsymbol{\mu}_{\boldsymbol{p},K} \to 0$$

where $\boldsymbol{\mu}_{\boldsymbol{p},K}$ denotes the multiplicative group of the p roots of unity over K. So to compute Hopf orders in $K(C_p \times C_p)$ (including those of Elder type) we ought to compute the group of extensions $\operatorname{Ext}^1(\operatorname{Spec} H(i), \operatorname{Spec} H(j))$.

Unfortunately, the direct computation of this group is too difficult. The problem is somewhat easier if we consider the linear duals of $H(i)$ and $H(j)$.

In this paper we compute the elements in $\operatorname{Ext}^1(\operatorname{Spec} H(j)^*, \operatorname{Spec} H(i)^*)$ which over K appear as

$$0 \to \mathbf{C}_{p,K} \to \mathbf{C}_{p,K} \times \mathbf{C}_{p,K} \to \mathbf{C}_{p,K} \to 0,$$

where $\mathbf{C}_{p,K}$ is the constant group scheme of C_p over K. These are the generically trivial extensions, denoted as $\operatorname{Ext}^1_{gt}(\operatorname{Spec} H(j)^*, \operatorname{Spec} H(i)^*)$. We then compute the representing algebras of the middle terms of these generically trivial extensions, take their duals, and show that these duals are Elder orders in $K(C_p \times C_p)$. We follow the method of C. Greither [3, Part I] where the author has solved the analogous problem in the characteristic 0 case. Here is our main result (Proposition 3.9.)

Main Theorem. *Let H be an arbitrary R-Hopf order in $K(C_p \times C_p)$ that induces the short exact sequence*

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

Then H is an Elder order in $K(C_p \times C_p)$.

We begin with some preliminary results concerning the Larson order $H(i)$.

2. Larson Orders in KC_p

Let G be a finite group of order n whose elements are listed as $1 = g_0, g_1, \ldots, g_{n-1}$. Let T be a commutative ring with unity. Then the group ring TG is a T-Hopf algebra with comultiplication $\Delta_{TG} : TG \to TG \otimes_T TG$ defined as $g_k \mapsto g_k \otimes g_k$, counit $\epsilon_{TG} : TG \to T$ defined by $g_k \mapsto 1$ and coinverse $S_{TG} : TG \to TG$ given by $g_k \mapsto g_k^{-1}$, for $0 \le k \le n-1$. Note that $B = \{g_0, g_1, \ldots, g_{n-1}\}$ is a T-basis for

TG. Let $TG^* = \mathrm{Hom}_T(TG, T)$ denote the T-module of T-linear maps $TG \to T$ (the linear dual of TG.) Let $\{e_0, e_1, \ldots, e_{n-1}\}$ be the basis of TG^* dual to the basis B, that is, $\langle e_l, g_k\rangle = e_l(g_k) = \delta_{l,k}$, with

$$\langle\ ,\ \rangle : TG^* \times TG \to T$$

the duality map.

Proposition 2.1. *TG^* is a T-Hopf algebra.*

Proof. The T-algebra structure of TG^* is induced from the T-coalgebra structure of TG: the dual basis $\{e_0, e_1, \ldots, e_{n-1}\}$ is a collection of minimal idempotents and consequently

$$TG^* = \bigoplus_{m=0}^{n-1} Te_m \cong T^n,$$

as T-algebras. The T-coalgebra structure of TG^* is induced from the T-algebra structure of TG: comultiplication is defined by

$$\Delta_{TG^*}(e_m) = \sum_{g_m = g_a g_b} e_a \otimes e_b$$

and the counit map is defined as $\epsilon_{TG^*}(e_m) = \delta_{m,0}$. The coinverse map for TG^* is the transpose of the coinverse of TG, and is given by $S_{TG^*}(e_m) = e_n$ with $g_n = g_m^{-1}$, cf. [1, §1.4].

□

Applying Proposition 2.1 to the case $T = K$, $G = C_p$, we see that KC_p^* is a K-Hopf algebra. Let $H(i) = R\left[\frac{\sigma-1}{t^i}\right]$, $i \geq 0$, be a Larson order in KC_p and let $H(i)^* = \mathrm{Hom}_R(H(i), R)$ denote the R-module of R-linear maps $H(i) \to R$, the linear dual of $H(i)$.

Proposition 2.2. *For $i \geq 0$, $H(i)^* = R\left[\frac{\sigma-1}{t^i}\right]^*$ is an R-Hopf order in KC_p^*.*

Proof. Since $H(i) = R\left[\frac{\sigma-1}{t^i}\right]$ is an R-submodule of KC_p, free of rank p over R, $H(i)^* = R\left[\frac{\sigma-1}{t^i}\right]^*$ is an R-submodule of KC_p^*, free of rank p over R. Morover, since $H(i)$ is invariant under the comultiplication of KC_p, $H(i)^*$ is closed under the multiplication of KC_p^*. Moreover, $KH(i)^* = KC_p^*$, and so $H(i)^*$ is an R-order in KC_p^*.

Furthermore, since $H(i)$ is closed under the multiplication of KC_p, $H(i)^*$ is invariant under the comultiplication of KC_p^*. Thus $H(i)^*$ is an R-Hopf order in KC_p^*.

□

Proposition 2.3. *For $i \geq 0$, $H(i)^* = R\left[\frac{\sigma-1}{t^i}\right]^*$ is an R-Hopf algebra with Hopf algebra structure induced from KC_p^*.*

Proof. From Proposition 2.2, we know that $H(i)^*$ is an R-algebra. Since $H(i)^*$ is an R-Hopf order in KC_p^*, the comultiplication for $H(i)^*$ is the restriction of $\Delta_{KC_{p^*}}$ to $H(i)^*$. Since the counit map $\epsilon_{KC_p^*}$ is the transpose of the unit map λ_{KC_p}, the counit map $\epsilon_{KC_p^*}$ restricts to give a map $H(i)^* \to R$, which we take to be the counit map of $H(i)^*$. Since the coinverse map $S_{KC_p^*}$ is the transpose of the coinverse map S_{KC_p}, the coinverse map restricts to give a map $H(i)^* \to H(i)^*$, which we take to be the coinverse of $H(i)^*$. Thus $H(i)^*$ is an R-Hopf algebra with structure maps induced from KC_p^*. □

One has an inclusion

$$RC_p = R[\sigma - 1] \subseteq R\left[\frac{\sigma - 1}{t^i}\right],$$

and so there is an inclusion of linear duals

$$R\left[\frac{\sigma - 1}{t^i}\right]^* \subseteq RC_p^*.$$

By Proposition 2.1, $RC_p^* = \bigoplus_{m=0}^{p-1} Re_m \cong R^p$, and so $H(i)^* \subseteq \bigoplus_{m=0}^{p-1} Re_m \cong R^p$. An R-basis for $R\left[\frac{\sigma-1}{t^i}\right]^*$ can therefore be obtained in terms of the e_m.

There is a symmetric non-degenerate bilinear form on KC_p^*

$$B : KC_p^* \times KC_p^* \to K$$

defined as $B(x, y) = \sum_{m=0}^{p-1} \sigma^m(xy)$. Here σ^m is considered as an element of the double dual $KC_p^{**} = KC_p$. For an R-order A in KC_{p^*}, free of rank p on the basis $\{b_1, b_2, \dots, b_p\}$, we define

$$\operatorname{disc}(A/R) = R \det(B(b_m, b_n)).$$

Proposition 2.4. *An R-basis for $H(i)^* = R\left[\frac{\sigma-1}{t^i}\right]^*$ is of the form $\{1, \beta, \beta^2, \dots, \beta^{p-1}\}$ where*

$$\beta = t^i e_1 + 2t^i e_2 + \cdots + (p-1)t^i e_{p-1}.$$

Thus $H(i)^* = R[\beta]$ with $\beta^p = t^{(p-1)i}\beta$.

Proof. An R-basis for $H(i) = R\left[\frac{\sigma-1}{t^i}\right]$ is

$$\left\{1, \frac{\sigma - 1}{t^i}, \left(\frac{\sigma - 1}{t^i}\right)^2, \dots, \left(\frac{\sigma - 1}{t^i}\right)^{p-1}\right\}.$$

For $0 \le k, l \le p - 1$, let

$$v_{k,l} = \begin{cases} \binom{k}{l} t^{li} & \text{if } k \ge l \\ 0 & \text{if } k < l. \end{cases}$$

Then

$$\left\langle v_{0,k}e_0 + v_{1,k}e_1 + \cdots + v_{p-1,k}e_{p-1}, \left(\frac{\sigma - 1}{t^i}\right)^l \right\rangle = \delta_{k,l}.$$

Thus, with respect to the basis $E = \{e_0, e_1, \dots, e_{p-1}\}$ for RC_p^*, $H(i)^*$ has a basis consisting of the columns of the $p \times p$ matrix

$$M_E = \begin{pmatrix} \binom{0}{0} & 0 & 0 & 0 & 0 & \cdots & 0 \\ \binom{1}{0} & \binom{1}{1}t^i & 0 & 0 & 0 & \cdots & 0 \\ \binom{2}{0} & \binom{2}{1}t^i & \binom{2}{2}t^{2i} & 0 & 0 & \cdots & 0 \\ & \vdots & & & \ddots & & \vdots \\ \binom{p-1}{0} & \binom{p-1}{1}t^i & \binom{p-1}{2}t^{2i} & \cdots & & \cdots & \binom{p-1}{p-1}t^{(p-1)i} \end{pmatrix}.$$

Put

$$\begin{aligned} \beta &= \binom{1}{1}t^ie_1 + \binom{2}{1}t^ie_2 + \cdots + \binom{p-1}{1}t^ie_{p-1} \\ &= t^ie_1 + 2t^ie_2 + \cdots + (p-1)t^ie_{p-1}. \end{aligned}$$

Now, $\beta^p = t^{(p-1)i}\beta$. We claim that $R[\beta] = H(i)^*$. Certainly, $R[\beta] \subseteq H(i)^*$. We show equality by showing that

$$\operatorname{disc}(H(i)^*/R) = \operatorname{disc}(R[\beta]/R).$$

Note that $\operatorname{disc}(RC_p^*/R) = R$. One has that the module index

$$\begin{aligned} [RC_p^* : H(i)^*] &= R\det(M_E^T) \\ &= Rt^{(1+2+\cdots+(p-1))i} \\ &= Rt^{p(p-1)i/2}, \end{aligned}$$

and so,

$$\begin{aligned} \operatorname{disc}(H(i)^*/R) &= [RC_p^* : H(i)^*]^2\operatorname{disc}(RC_p^*/R) \\ &= Rt^{p(p-1)i}. \end{aligned}$$

On the other hand, $\{1, \beta, \beta^2, \dots, \beta^{p-1}\}$ is a an R-basis for $R[\beta]$ and its basis matrix with respect to E is

$$N_E = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & t^i & (t^i)^2 & \cdots & (t^i)^{p-1} \\ 1 & 2t^i & (2t^i)^2 & \cdots & (2t^i)^{p-1} \\ & \vdots & & & \vdots \\ 1 & (p-1)t^i & ((p-1)t^i)^2 & \cdots & ((p-1)t^i)^{p-1} \end{pmatrix}.$$

Since N_E is Vandermonde,

$$\begin{aligned} \det(N_E) &= \prod_{k=1}^{p-1}\prod_{l=0}^{p-k-1}((p-k)t^i - lt^i) \\ &= t^{((p-1)+(p-2)+\cdots+2+1)i}\prod_{k=1}^{p-1}\prod_{l=0}^{p-k-1}(p-k-l) \\ &= qt^{p(p-1)i/2} \end{aligned}$$

where q is an integer not divisible by p. Consequently,

$$\begin{aligned} \operatorname{disc}(R[\beta]/R) &= [RC_p^* : R[\beta]]^2 \operatorname{disc}(RC_p^*/R) \\ &= Rt^{p(p-1)i} \\ &= \operatorname{disc}(H(i)^*). \end{aligned}$$

□

Proposition 2.5. *The Hopf algebra structure of $H(i)^* = R[\beta]$, $\beta^p = t^{(p-1)i}\beta$, is given by $\Delta_{KC_p^*}(\beta) = 1\otimes\beta + \beta\otimes 1$, $\epsilon_{KC_p^*}(\beta) = 0$, and $S_{KC_p^*}(\beta) = -\beta$.*

Proof. Let $\Delta = \Delta_{KC_p^*}$. By direct computation, one has

$$\begin{aligned} \Delta_{KC_p^*}(\beta) &= t^i\Delta(e_1) + 2t^i\Delta(e_2) + \cdots + (p-1)t^i\Delta(e_{p-1}) \\ &= t^i\left(\sum_{\sigma=\sigma^a\sigma^b}\sigma^a\otimes\sigma^b\right) + 2t^i\left(\sum_{\sigma^2=\sigma^a\sigma^b}\sigma^a\otimes\sigma^b\right) \\ &\quad + \cdots + (p-1)t^i\left(\sum_{\sigma^{p-1}=\sigma^a\sigma^b}\sigma^a\otimes\sigma^b\right) \\ &= (e_0+e_1+\cdots+e_{p-1})\otimes(t^ie_1+2t^ie_2+\cdots+(p-1)t^ie_{p-1}) \\ &\quad + (t^ie_1+2t^ie_2+\cdots+(p-1)t^ie_{p-1})\otimes(e_0+e_1+\cdots+e_{p-1}) \\ &= 1\otimes\beta+\beta\otimes 1. \end{aligned}$$

Moreover, as one can check, $\epsilon_{KC_p^*}(\beta) = 0$, and $S_{KC_p^*}(\beta) = -\beta$. □

Let X be an indeterminate. The ring of polynomials $R[X]$ is R-Hopf algebra with comultiplication defined by $\Delta_{R[X]}(X) = 1 \otimes X + X \otimes 1$, counit defined by $\epsilon_{R[X]}(X) = 0$ and coinverse given by $S_{K[X]}(X) = -X$. The R-Hopf algebra $R[X]$ corresponds to the R-group scheme $\mathbf{G}_a = \operatorname{Spec} R[X]$, the additive R-group scheme. Let $\psi(X) = X^p - t^{(p-1)i}X$. The map $\psi : R[X] \to R[X]$ is a homomorphism of R-Hopf algebras corresponding to a homomorphism of R-group schemes

$$\Psi : \mathbf{G}_a \to \mathbf{G}_a,$$

defined as follows. For each commutative R-algebra A, $g \in \mathbf{G}_a(A)$, $g(X) = a$, $a \in A$,

$$\begin{aligned} \Psi_A(g)(X) &= g(\psi(X)) \\ &= g(X^p - t^{(p-1)i}X) \\ &= g(X)^p - t^{(p-1)i}g(X) \\ &= a^p - t^{(p-1)i}a. \end{aligned}$$

Observe that there is an isomorphism of R-Hopf algebras

$$R[X]/(\psi(X)) \to H(i)^*,$$

defined as $X \mapsto \beta$. Thus the kernel of Ψ is a subgroup scheme represented by $H(i)^*$. One has an exact sequence of R-group schemes,

$$0 \to \operatorname{Spec} H(i)^* \to \mathbf{G}_a \xrightarrow{\Psi} \mathbf{G}_a.$$

In fact, in the faithfully flat topology we can say a bit more.

Proposition 2.6. *There is a short exact sequence*

$$0 \to \mathit{Spec}\, H(i)^* \to \mathbf{G}_a \xrightarrow{\Psi} \mathbf{G}_a \to 0 \tag{2}$$

in the faithfully flat topology.

Proof. Let A be a commutative R-algebra and let $y \in \mathbf{G}_a(A)$ be defined as $y : X \mapsto a$, $a \in A$. Let α be a root of $\psi(X) - a$ in some ring extension B of A. Then $\varrho : A \to B$ is a faithfully flat map of R-algebras. Let $y' = \varrho y \in \mathbf{G}_a(B)$. Now the element $x \in \mathbf{G}_a(B)$ defined by $x : X \mapsto \alpha$ is so that $\Psi_B(x) = y'$. Indeed,

$$\begin{aligned} \Psi_B(x)(X) &= x(\psi(X)) \\ &= \psi(x(X)) \\ &= \psi(\alpha) \\ &= a. \end{aligned}$$

Thus Ψ is an epimorphism in the faithfully flat topology.

□

We shall employ short exact sequence (2) in what follows.

3. Computation of Extensions

Let $i, j \geq 0$ be integers and let $H(i)^* = R[\frac{\sigma-1}{t^i}]^*$ and $H(j)^* = R[\frac{\tau-1}{t^j}]^*$ be R-Hopf orders in KC_p^* corresponding to R-group schemes $\operatorname{Spec} H(i)^*$ and $\operatorname{Spec} H(j)^*$, respectively. We are interested in computing all short exact sequences of the form

$$0 \to \operatorname{Spec} H(i)^* \to \mathbf{G} \to \operatorname{Spec} H(j)^* \to 0$$

where $\mathbf{G}$ is an R-group scheme. In other words, we seek to calculate the group $\operatorname{Ext}^1(\operatorname{Spec} H(j)^*, \operatorname{Spec} H(i)^*)$ of 1-extensions of $\operatorname{Spec} H(i)^*$ by $\operatorname{Spec} H(j)^*$.

Since there are obstructions to this calculation, we proceed indirectly by computing $\operatorname{Ext}^1(\operatorname{Spec} H(j)^*, \mathbf{G}_a)$, $\mathbf{G}_a = \operatorname{Spec} R[X]$. Note that over K these extensions appear as

$$0 \to \mathbf{G}_{a,K} \to \mathbf{G}_{a,K} \times_t \mathbf{C}_{p,K} \to \mathbf{C}_{p,K} \to 0,$$

with $\mathbf{G}_{a,K} = \operatorname{Spec} K[X]$ and $\mathbf{C}_{p,K} = \operatorname{Spec} KC_p^*$, the constant group scheme of C_p. By $\times_t$ we mean that the cartesian product is twisted in some manner. The group $\operatorname{Ext}^1(\operatorname{Spec} H(j)^*, \mathbf{G}_a)$ is computed in the usual way "cocycles modulo coboundaries":

$$\operatorname{Ext}^1(\operatorname{Spec} H(j)^*, \mathbf{G}_a) = C(\operatorname{Spec} H(j)^*, \mathbf{G}_a)/B(\operatorname{Spec} H(j)^*, \mathbf{G}_a),$$

where

$$\begin{aligned} C(\operatorname{Spec} H(j)^*, \mathbf{G}_a) &= \{f \in \operatorname{Nat}(\operatorname{Spec} H(j)^* \times \operatorname{Spec} H(j)^* \to \mathbf{G}_a) \\ &\quad : \ f \text{ is a cocycle}\}. \end{aligned}$$

By cocycle, we mean that for all commutative R-algebras A and $x, y, z \in \operatorname{Spec} H(j)^*(A)$,

$$f_A(x,y)(X) + f_A(x+y,z)(X) = f_A(y,z)(X) + f_A(x,y+z)(X), \quad (3)$$

$$f_A(x,0)(X) = 0 = f_A(0,x)(X). \quad (4)$$

Coboundaries are certain cocycles defined as

$$B(\operatorname{Spec} H(j)^*, \mathbf{G}_a) = \{\partial g : \ g \in \operatorname{Nat}(\operatorname{Spec} H(j)^* \to \mathbf{G}_a), g_A(0) = 0\},$$

where

$$\partial g_A(x,y)(X) = g_A(x)(X) - g_A(x+y)(X) + g_A(y)(X).$$

The problem becomes: how do we characterize these sets of natural transformations? Let us consider coboundaries first. By Yoneda's Lemma, natural transformations $g : \operatorname{Spec} H(j)^* \to \mathbf{G}_a$ are in a 1-1 correspondence with R-algebra homomorphisms $\operatorname{Hom}_{R\text{-alg}}(R[X], H(j)^*)$. The R-algebra maps $R[X] \to H(j)^* = R[\frac{\tau-1}{t^j}]^*$ are of the form $X \mapsto a$, with $a \in H(j)^*$. Since $H(j)^* \subseteq \bigoplus_{m=0}^{p-1} Re_m \cong R^p$, we can write $a \in H(j)^*$ as a R-linear combination $a = a_0e_0 + a_1e_1 + \cdots + a_{p-1}e_{p-1}$. Note that $a = \sum_{m=0}^{p-1} a_m e_m \in R[\frac{\tau-1}{t^j}]^*$ if and only if

$$\left\langle a_0e_0 + a_1e_1 + \cdots + a_{p-1}e_{p-1}, \left(\frac{\tau-1}{t^j}\right)^k \right\rangle \in R,$$

for all $0 \le k \le p-1$. That is, $a = \sum_{m=0}^{p-1} a_m e_m \in R[\frac{\tau-1}{t^j}]^*$ if and only if the kth iterated difference d^k satisfies

$$d^k(a) = \sum_{m=0}^{k} \binom{k}{m} (-1)^m a_{k-m} \in t^{kj}R,$$

for all $0 \le k \le p-1$.

So coboundaries are cocycles of the form ∂g where $g : \operatorname{Spec} H(j)^* \to \mathbf{G}_a$ is a natural transformation and g corresponds to an algebra map $R[X] \to H(j)^*$ given by $X \mapsto a = \sum_{m=0}^{p-1} a_m e_m \in H(j)^*$ with $a_0 = 0$.

We can characterize cocycles in a similar way. Cocycles consist of natural transformations

$$f \in \operatorname{Nat}(\operatorname{Spec} H(j)^* \times \operatorname{Spec} H(j)^* \to \mathbf{G}_a)$$

that satisfy the cocycle conditions (3), (4). By Yoneda's Lemma, these natural transformations are in a 1-1 correspondence with R-algebra maps

$$R[X] \to H(j)^* \otimes_R H(j)^*$$

of the form $X \mapsto b$, with $b \in H(j)^* \otimes_R H(j)^*$. Since

$$H(j)^* \otimes_R H(j)^* \subseteq RC_p^* \otimes_R RC_p^* = \bigoplus_{m=0}^{p-1} Re_m \otimes_R \bigoplus_{n=0}^{p-1} Re_n,$$

and $\{e_m \otimes e_n\}$ is an R-basis for $RC_p^* \otimes_R RC_p^*$, the element b can be written as an R-linear combination of the $e_m \otimes e_n$. Thus the algebra maps are given as

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

with $a_{m,n} \in R$. Note that the element $b = \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} a_{m,n}(e_m \otimes e_n)$, $a_{m,n} \in R$, is in $H(j)^* \otimes_R H(j)^*$ if and only if the double iterated difference $d^{k,k'}$satisfies

$$d^{k,k'}(b) = \sum_{m=0}^{k} \sum_{n=0}^{k'} \binom{k}{m} \binom{k'}{n} (-1)^{m+n} a_{k-m,k'-n} \in t^{(k+k')i} R,$$

for all $0 \leq k, k' \leq p-1$.

Let $f : \operatorname{Spec} H(j)^* \times \operatorname{Spec} H(j)^* \to \mathbf{G}_a$ be a natural transformation corresponding to the algebra map $\phi_f : R[X] \to H(j)^* \otimes_R H(j)^*$, defined as

$$\phi_f : X \mapsto b = \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} a_{m,n}(e_m \otimes e_n),$$

$a_{m,n} \in R$. The group $\operatorname{Spec} H(j)^*(R)$ consists of p elements

$$x_m : \beta \mapsto m t^j,$$

$0 \leq m \leq p-1$, and hence, $\operatorname{Spec} H(j)^*(R) = \mathbb{Z}/p\mathbb{Z}$. Also, $\mathbf{G}_a(R) = R$. Thus f_R is a function

$$f_R : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to R.$$

Let $x_m, x_n \in \operatorname{Spec} H(j)^*(R)$. Then

$$\begin{aligned} f_R(x_m, x_n)(X) &= (x_m \otimes x_n)(\phi_f(X)) \\ &= (x_m \otimes x_n)\Big(\sum_{m'=0}^{p-1} \sum_{n'=0}^{p-1} a_{m',n'}(e_{m'} \otimes e_{n'})\Big) \\ &= a_{m,n}. \end{aligned}$$

In this way, f determines a function

$$\hat{f} : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to R$$

defined as $\hat{f}(x_m, x_n) = a_{m,n}$.

Next, let $g : \operatorname{Spec} H(j)^* \to \mathbf{G}_a$ be a natural transformation corresponding to the algebra map $\phi_g : R[X] \to H(j)^*$, defined as

$$\phi_g : X \mapsto a = \sum_{m=0}^{p-1} a_m e_m,$$

$a_m \in R$. Let $x_m \in \operatorname{Spec} H(j)^*(R)$. Then

$$\begin{aligned} g_R(x_m)(X) &= x_m(\phi_g(X)) \\ &= x_m(\sum_{m'=0}^{p-1} a_{m'}e_{m'}) \\ &= a_m. \end{aligned}$$

And so, g determines a function

$$\hat{g} : \mathbb{Z}/p\mathbb{Z} \to R$$

defined as $\hat{g}(x_m) = a_m$. In what follows we consider the familiar construction of extensions of R by $\mathbb{Z}/p\mathbb{Z}$,

$$\mathrm{Ext}^1(\mathbb{Z}/p\mathbb{Z}, R) = C(\mathbb{Z}/p\mathbb{Z}, R)/B(\mathbb{Z}/p\mathbb{Z}, R),$$

where $C(\mathbb{Z}/p\mathbb{Z}, R)$ is the set of all functons $f : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to R$ that satisfy

$$f(l, m) + f(l + m, n) = f(m, n) + f(l, m + n),$$

$$f(m, 0) = 0 = f(0, n),$$

for all $l, m, n \in \mathbb{Z}/p\mathbb{Z}$, (cocycles) and $B(\mathbb{Z}/p\mathbb{Z}, R)$ consists of those cocycles of the form ∂g for some function $g : \mathbb{Z}/p\mathbb{Z} \to R$, $g(0) = 0$, where

$$\partial g(m, n) = g(m) - g(m + n) + g(n),$$

for all $m, n \in \mathbb{Z}/p\mathbb{Z}$.

Proposition 3.1. *Let $f \in Nat(Spec\, H(j)^* \times Spec\, H(j)^* \to \mathbf{G}_a)$. Then f is a cocycle in $C(Spec\, H(j)^*, \mathbf{G}_a)$ if and only if $\hat{f}$ is a cocycle in $C(\mathbb{Z}/p\mathbb{Z}, R)$.*

Proof. Suppose $f : \mathrm{Spec}\, H(j)^* \times \mathrm{Spec}\, H(j)^* \to \mathbf{G}_a$ is a cocycle, with corresponding algebra homomorphism

$$\phi_f : X \mapsto b = \sum_{m'=0}^{p-1} \sum_{n'=0}^{p-1} a_{m',n'}(e_{m'} \otimes e_{n'}).$$

Then for all $x_l, x_m, x_n \in \mathrm{Spec}\, H(j)^*(R)$,

$$f_R(x_l, x_m)(X)+f_R(x_l+x_m, x_n)(X) = f_R(x_m, x_n)(X)+f_R(x_l, x_m+x_n)(X).$$

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

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

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

$$\hat{f}(x_l, x_m) + \hat{f}(x_{l+m}, x_n) = \hat{f}(x_m, x_n) + \hat{f}(x_l, x_{m+n}).$$

Moreover,

$$f_R(x_l, 0)(X) = 0 = f_R(0, x_m)(X)$$

for all $x_l, x_m \in \operatorname{Spec} H(j)^*(R)$. Thus for all $0 \le l, m \le p-1$,

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

and so,

$$\hat{f}(x_l, 0) = 0 = \hat{f}(0, x_m).$$

It follows that $\hat{f}$ is in $C(\mathbb{Z}/p\mathbb{Z}, R)$.

For the converse, suppose that $\hat{f} : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to R$ is a cocycle obtained from the natural transformation $f : \operatorname{Spec} H(j)^* \times \operatorname{Spec} H(j)^* \to \mathbf{G}_a$. Then for all $0 \le l, m, n \le p-1$ 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,

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

Consequently, with $\Delta = \Delta_{H(j)^*}$,

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

Thus, for any R-algebra A and $x, y, z \in \operatorname{Spec} H(j)^*(A)$.

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

which implies

$$(x\otimes y)\phi_f(X) + ((x+y)\otimes z)\phi_f(X) = (y\otimes z)\phi_f(X) + (x\otimes(y+z))\phi_f(X).$$

Thus

$$f_A(x,y)(X) + f_A(x+y,z)(X) = f_A(y,z)(X) + f_A(x,y+z)(X).$$

Now, suppose $0 = a_{m',0}$, for $m' = 0,\ldots,p-1$, and let $x \in \operatorname{Spec} H(j)^*(A)$. Then

$$\begin{aligned} 0 &= (x \otimes \lambda_A \epsilon_{H(j)^*})(\sum_{m'=0}^{p-1}\sum_{n'=0}^{p-1} a_{m',n'}(e_{m'} \otimes e_{n'})) \\ &= (x \otimes 0)(\sum_{m'=0}^{p-1}\sum_{n'=0}^{p-1} a_{m',n'}(e_{m'} \otimes e_{n'})) \\ &= (x \otimes 0)\phi_f(X) \\ &= f_A(x,0)(X). \end{aligned}$$

In a similar manner, the condition $0 = a_{0,n}$, for $n = 0,\ldots,p-1$, yields $f_A(0,y)(X) = 0$ for $y \in \operatorname{Spec} H(j)^*(A)$. Consequently, f satisfies the cocycle conditions (3), (4).

□

Proposition 3.2. *Let $f \in C(\mathit{Spec}\, H(j)^*, \mathbf{G}_a)$. Then $f \in B(\mathit{Spec}\, H(j)^*, \mathbf{G}_a)$ if and only if $\hat{f} = \partial\hat{g}$ for some natural transformation $g : \mathit{Spec}\, H(j)^* \to \mathbf{G}_a$ with $g_A(0) = 0$ for all commutative R-algebras A.*

Proof. Let $f \in B(\operatorname{Spec} H(j)^*, \mathbf{G}_a)$. Then there exists a natural transformation $g : SpH(j)^* \to \mathbf{G}_a$ for which

$$f_R(x_m, x_n)(X) = g_R(x_m)(X) - g_R(x_m + x_n)(X) + g_R(x_n)(X) \tag{5}$$

and $g_A(0) = 0$ for all commutative R-algebras A. Let

$$\phi_f : X \to \sum_{m=0}^{p-1}\sum_{n=0}^{p-1} a_{m,n}(e_m \otimes e_n),$$

and $\phi_g : X \mapsto \sum_{m=0}^{p-1} a_m$ denote the algebra maps corresponding to f, g, respectively. From (5) we obtain

$$a_{m,n} = a_m - a_{m+n} + a_m,$$

for all $0 \le m,n \le p-1$ ($m+n$ taken modulo p.) It follows that $\hat{f} = \partial\hat{g}$.

For the converse suppose that $\hat{f} = \partial\hat{g}$ for some natural transformation $g : SpH(j)^* \to \mathbf{G}_a$ with $g_A(0) = 0$. Then

$$a_{m,n} = a_m - a_{m+n} + a_n,$$

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

$$\begin{aligned}\sum_{m,n=0}^{p-1} a_{m,n}(e_m \otimes e_n) &= \sum_{m,n=0}^{p-1} (a_m - a_{m+n} + a_n)(e_m \otimes e_n) \\ &= \sum_{m=0}^{p-1} a_m(e_m \otimes 1) - \sum_{k=0}^{p-1} a_k \Delta_{H(j)^*}(e_k) + \sum_{n=0}^{p-1} a_n(1 \otimes e_n).\end{aligned} \tag{6}$$

Let $x, y \in \operatorname{Spec} H(j)^*(A)$. Then (6) implies that

$$\begin{aligned}&(x \otimes y) \sum_{m,n=0}^{p-1} a_{m,n}(e_m \otimes e_n) \\ &= (x \otimes y) \sum_{m=0}^{p-1} a_m(e_m \otimes 1) - (x \otimes y) \sum_{k=0}^{p-1} \Delta_{H(j)^*}(a_k e_k) + (x \otimes y) \sum_{n=0}^{p-1} a_n(1 \otimes e_n),\end{aligned}$$

and so,

$$(x \otimes y)\phi_f(X) = x(\phi_g(X)) - (x+y)(\phi_g(X)) + y(\phi_g(X)).$$

Thus

$$f_A(x,y)(X) = g_A(x)(X) - g_A(x+y)(X) + g_A(y)(X),$$

and so, $f = \partial g$.

□

Define:

$\hat{C} = \{r \in C(\mathbb{Z}/p\mathbb{Z}, R) :\ r = \hat{f}$ for some natural transformation $f : \operatorname{Spec} H(j)^* \times \operatorname{Spec} H(j)^* \to \mathbf{G}_a\}$.

$\hat{B} = \{r \in \hat{C} :\ r = \partial \hat{g}$ for some natural transformation $g : \operatorname{Spec} H(j)^* \to \mathbf{G}_a$ with $g_A(0) = 0$ for all commutative R-algebras $A\}$.

Proposition 3.3. *$Ext^1(Spec\, H(j)^*, \mathbf{G}_a) = \hat{C}/\hat{B}$.*

Proof. This follows from Proposition 3.1 and Proposition 3.2. □

A cocycle in $r : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to R$ in $\hat{C}$ will be given as the $p \times p$ matrix

$$M_r = \begin{pmatrix} a_{0,0} & a_{0,1} & \cdots & \cdots & a_{0,p-1} \\ a_{1,0} & a_{1,1} & \cdots & \cdots & a_{1,p-1} \\ \vdots & \vdots & & & \vdots \\ a_{p-1,0} & a_{p-1,1} & \cdots & \cdots & a_{p-1,p-1} \end{pmatrix}.$$

with $r(x_m, x_n) = a_{m,n}$.

Proposition 3.4. *A cocycle $r \in \hat{C}$ is congruent modulo $\hat{B}$ to a cocycle of the form*

$$M_w = \begin{pmatrix} 0 & 0 & \cdots & & \cdots & 0 \\ 0 & 0 & \cdots & & 0 & w \\ 0 & 0 & \cdots & 0 & w & w \\ \vdots & \vdots & & & & \vdots \\ \vdots & 0 & & & & \vdots \\ 0 & w & w & & \cdots & w \end{pmatrix}$$

for some $w \in R$.

Proof. Let $r \in \hat{C}$. Then $r = \hat{f}$ for some natural transformation f : $\operatorname{Spec} H(j)^* \times \operatorname{Spec} H(j)^* \to \mathbf{G}_a$. The matrix of $\hat{f}$ has the form

$$M_{\hat{f}} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & a_{1,1} & a_{1,2} & \cdots & a_{1,p-1} \\ 0 & a_{2,1} & a_{2,2} & \cdots & a_{2,p-1} \\ \vdots & \vdots & \vdots & & \vdots \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & a_{p-1,1} & a_{p-1,2} & \cdots & a_{p-1,p-1} \end{pmatrix},$$

for elements $a_{m,n} \in R$. $M_{\hat{f}}$ is symmetric. Since

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

$$\left\langle \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} a_{m,n}(e_m \otimes e_n), (\tau - 1)^k \otimes (\tau - 1)^{k'} \right\rangle \in t^{(k+k')j} R,$$

for $0 \leq k, k' \leq p-1$. In the second row of $M_{\hat{f}}$, let l be the smallest integer $\leq p-2$, for which $a_{1,l} \neq 0$. Now,

$$\left\langle \sum_{m=0}^{p-1}\sum_{n=0}^{p-1} a_{m,n}(e_m \otimes e_n), \tau - 1 \otimes (\tau-1)^l, \right\rangle = a_{1,l} \in t^{(1+l)j}R. \qquad (7)$$

Consider the element $c = \sum_{m=0}^{l+1} c_m e_m$ with

$$c_m = \begin{cases} 0 & \text{if } 0 \le m \le l \\ a_{1,l} & \text{if } m = l+1. \end{cases}$$

Now, $d^k(c) \in t^{kj}R$ for $0 \le k \le l+1$. And so, c satisfies the first $l+2$ conditions for membership in $H(j)^*$. Note that c has only $l+2$ components. However, one can find elements c_m, $m = l+2, l+3, \ldots, p-1$, so that $c = \sum_{m=0}^{p-1} c_m e_m \in H(j)^*$. Now, c corresponds to a natural transformation

$$s : \operatorname{Spec} H(j)^* \to \mathbf{G}_a, \quad s_A(0) = 0,$$

and a function $\hat{s} : \mathbb{Z}/p\mathbb{Z} \to R$. Thus $\partial\hat{s}$ is an element of $\hat{B}$ and $\hat{f} + \partial\hat{s}$ has matrix whose second row satisfies

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

Repeating this process, we find that $\hat{f}$ is congruent modulo $\hat{B}$ to a cocycle (also denoted as $\hat{f}$) with matrix

$$M_{\hat{f}} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & a_{1,p-1} \\ 0 & 0 & a_{2,2} & \cdots & a_{2,p-2} & a_{2,p-1} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & a_{p-2,2} & \cdots & & a_{p-2,p-1} \\ 0 & a_{p-1,1} & a_{p-1,2} & \cdots & a_{p-1,p-2} & a_{p-1,p-1} \end{pmatrix}.$$

The cocycle conditions (3), (4) then imply that $\hat{f}$ is congruent modulo $\hat{B}$ to a cocycle in $\hat{C}$ with matrix

$$M_w = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & w \\ 0 & \cdots & 0 & w & w \\ \vdots & & \vdots & & \vdots \\ 0 & w & w & \cdots & w \end{pmatrix},$$

for $w \in R$, cf. [3, Theorem 3.4], [4, Proposition 8.2.3].

□

Proposition 3.5. *$Ext^1(Spec\, H(j)^*, \mathbf{G}_a) \cong Rt^{pj}$.*

Proof. By Proposition 3.4, every coset in $\hat{C}/\hat{B}$ can be represented by a cocycle of the form M_w for some $w \in R$. Now, a matrix of the form M_w corresponds to a cocycle in $\hat{C}$ if and only if $d^{k,k'}(M_w) \in Rt^{(k+k')j}$ for all $0 \leq k, k' \leq p-1$. And one finds that $d^{k,k'}(M_w) \in Rt^{(k+k')j}$ for all $0 \leq k, k' \leq p-1$, if and only if $w \in Rt^{pj}$.

Now, suppose that the cocycle $r \in \hat{C}$ with matrix M_w is of the form $r = \partial\hat{g}$ for some natural transformation $g : \mathrm{Spec}\, H(j)^* \to \mathbf{G}_a$, $g_A(0) = 0$. Let $\phi_g : X \mapsto a = \sum_{m=0} a_m e_m \in H(j)^*$ be the algebra map corresponding to g. Now, $r = \partial\hat{g}$ implies that

$$\begin{aligned} a_1 + a_1 - a_2 &= 0 \\ a_1 + a_2 - a_3 &= 0 \\ a_1 + a_3 - a_4 &= 0 \\ &\vdots \\ a_1 + a_{p-2} - a_{p-1} &= 0 \\ a_1 + a_{p-1} - a_0 &= w, \end{aligned}$$

hence $w = 0$.

□

Let

$$K \otimes_R - : \mathrm{Ext}^1(\mathrm{Spec}\, H(j)^*, \mathbf{G}_a) \to \mathrm{Ext}^1(\mathrm{Spec}\, KC_p^*, \mathbf{G}_{a,K})$$

be the maps that takes the extension

$$0 \to \mathbf{G}_a \to \mathbf{G} \to \mathrm{Spec}\, H(j)^* \to 0$$

to its "generic" extension over K:

$$0 \to \mathbf{G}_{a,K} \to K \otimes_R \mathbf{G} \to \mathrm{Spec}\, KC_p^* \to 0.$$

The kernel of $K \otimes_R -$ is the group of generically trivial extensions, denoted as $\mathrm{Ext}^1_{gt}(\mathrm{Spec}\, H(j)^*, \mathbf{G}_a)$. These are the extensions in $\mathrm{Ext}^1(\mathrm{Spec}\, H(j)^*, \mathbf{G}_a)$ that over K appear as

$$0 \to \mathbf{G}_{a,K} \to \mathbf{G}_{a,K} \times \mathbf{C}_p \to \mathbf{C}_p \to 0.$$

Proposition 3.6. *An element of $Ext^1_{gt}(Spec\, H(j)^*, \mathbf{G}_a)$ is of the form*

$$0 \to \mathbf{G}_a \to Spec\, R[X + a, \beta] \to Spec\, H(j)^* \to 0,$$

where $a = \eta e_1 + 2\eta e_2 + \cdots + (p-1)\eta e_{p-1}$ for some $\eta \in K$ and $\beta = t^j e_1 + 2t^j e_2 + \cdots + (p-1)t^j e_{p-1}$.

Proof. Let
$$0 \to \mathbf{G}_a \to \mathbf{G} \to \operatorname{Spec} H(j)^* \to 0$$
denote a generically trivial extension corresponding to the cocycle $f : \operatorname{Spec} H(j)^* \times \operatorname{Spec} H(j)^* \to \mathbf{G}_a$ whose matrix is M_w. The corresponding algebra map is $\phi_f : X \to M_w$. As a group scheme, $\mathbf{G} = \mathbf{G}_a \times \operatorname{Spec} H(j)^*$ with the multiplication twisted by the cocycle f. Over K, M_w corresponds to a cocycle

$$K \otimes f : \operatorname{Spec} KH(j)^* \times \operatorname{Spec} KH(j)^* \to \operatorname{Spec} K[X]$$
in $C(\operatorname{Spec} KH(j)^*, \operatorname{Spec} K[X])$ that is trivial. Thus, $K \otimes f = \partial g$, for some natural transformation $g : \operatorname{Spec} KH(j)^* \to \operatorname{Spec} K[X]$ and g corresponds to an algebra map $\phi_g : X \mapsto a$, for some $a = \sum_{m=0}^{p-1} a_m e_m \in KH(j)^*$. As shown above, this implies that $w = 0$. Moreover,
$$a = \eta e_1 + 2\eta e_2 + \cdots + (p-1)\eta e_{p-1},$$
for some $\eta \in K$ (actually, $\eta = a_1$.)

There is an isomorphism of K-group schemes
$$g' : \mathbf{G}_{a,K} \times \operatorname{Spec} KH(j)^* \to \operatorname{Spec} K[X] \times \operatorname{Spec} KC_p^*$$
defined by
$$g'(x, y) = (x + g(y), y),$$
for $x \in \mathbf{G}_{a,K}$, $y \in \operatorname{Spec} KH(j)^*$. The isomorphism g' makes the following diagram commute:

$$\begin{array}{ccccccccc}
0 & \to & \operatorname{Spec} K[X] & \to & \mathbf{G}_{a,K} \times \operatorname{Spec} KH(j)^* & \to & \operatorname{Spec} KH(j)^* & \to & 0 \\
 & & || & & g' \downarrow & & || & & \\
0 & \to & \operatorname{Spec} K[X] & \to & \operatorname{Spec} K[X] \times \operatorname{Spec} KC_p^* & \to & \operatorname{Spec} KC_p^* & \to & 0
\end{array}$$

The Hopf algebra isomorphism corresponding to g' is
$$\psi : K[X] \otimes_K KC_p^* \to K[X] \otimes_K KH(j)^*,$$
defined as
$$X \otimes 1 \mapsto X \otimes 1 + 1 \otimes (\eta e_1 + 2\eta e_2 + \cdots + (p-1)\eta e_{p-1}),$$

$$1 \otimes \beta \mapsto 1 \otimes \beta,$$
with $KC_p^* = K[\beta], \beta^p = t^{(p-1)j}\beta$,
$$\beta = t^j e_1 + 2t^j e_2 + \cdots + (p-1)t^j e_{p-1}.$$

If we restrict the map ψ to $R[X] \otimes_R H(j)^*$ its image is

$$R\,[X \otimes 1 + 1 \otimes a, 1 \otimes \beta] \cong R\,[X + a, \beta]\,.$$

Thus

$$0 \to \operatorname{Spec} R[X] \to \operatorname{Spec} R[X + a, \beta] \to \operatorname{Spec} H(j)^* \to 0$$

is the generically trivial extension corresponding to the cocycle f.

$\square$

Let $\{e_{m,n}\}$, $0 \le m, n \le p-1$, be the basis for $K(C_p \times C_p)^*$ that is dual to the basis $\{(\sigma^c, \tau^d)\}$, $0 \le c, d \le p-1$ for $K(C_p \times C_p)$. We have $e_{m,n}((\sigma^a, \tau^b)) = \delta_{m,a}\delta_{n,b}$. Equivalently, $\langle e_{m,n}, (\sigma^a, \tau^b)\rangle = \delta_{m,a}\delta_{n,b}$, where $\langle\ ,\rangle : K(C_p \times C_p)^* \times K(C_p \times C_p) \to K$ is the duality map.

Proposition 3.7. *An element of $\mathit{Ext}^1_{gt}(\mathit{Spec}\, H(j)^*, \mathit{Spec}\, H(i)^*)$ can be written in the form*

$$0 \to \mathit{Spec}\, H(i)^* \to \mathit{Spec}\, R[\gamma + a, \beta] \to \mathit{Spec}\, H(j)^* \to 0,$$

where

$$\begin{aligned} a &= \eta(e_{0,1} + e_{1,1} + \cdots + e_{p-1,1}) + 2\eta(e_{0,2} + e_{1,2} + \cdots + e_{p-1,2}) \\ &\quad + \cdots + (p-1)\eta(e_{0,p-1} + e_{1,p-1} + \cdots + e_{p-1,p-1}), \end{aligned}$$

$$\begin{aligned} \beta &= t^j(e_{0,1} + e_{1,1} + \cdots + e_{p-1,1}) + 2t^j(e_{0,2} + e_{1,2} + \cdots + e_{p-1,2}) \\ &\quad + \cdots + (p-1)t^j(e_{0,p-1} + e_{1,p-1} + \cdots + e_{p-1,p-1}), \end{aligned}$$

$$\begin{aligned} \gamma &= t^i(e_{1,0} + e_{1,1} + \cdots + e_{1,p-1}) + 2t^i(e_{2,0} + e_{2,1} + \cdots + e_{2,p-1}) \\ &\quad + \cdots + (p-1)t^i(e_{p-1,0} + e_{p-1,1} + \cdots + e_{p-1,p-1}). \end{aligned}$$

Proof. Recall the short exact sequence in the faithfully flat topology (Proposition 2.6)

$$0 \to \operatorname{Spec} H(i)^* \to \mathbf{G}_a \xrightarrow{\Psi} \mathbf{G}_a \to 0 \tag{8}$$

with Ψ given by the Hopf map

$$\psi : R[X] \to R[X],$$

$\psi(X) = X^p - t^{(p-1)i}X$. Applying (8) in the long exact sequence in cohomology yields the isomorphism

$\operatorname{Ext}^1_{gt}(\operatorname{Spec} H(j)^*, \operatorname{Spec} H(i)^*)$

$$\cong \ker(\mathrm{Ext}^1_{gt}(\mathrm{Spec}\, H(j)^*, \mathbf{G}_a) \xrightarrow{\Psi} \mathrm{Ext}^1_{gt}(\mathrm{Spec}\, H(j)^*, \mathbf{G}_a)), \tag{9}$$

cf. [3, Corollary 3.6b]. From the isomorphism (9) we conclude that an arbitrary element of $\mathrm{Ext}^1_{gt}(\mathrm{Spec}\, H(j)^*, \mathrm{Spec}\, H(i)^*)$ can be written as

$$\begin{aligned} 0 \to \mathrm{Spec}\,(R[X]/(\psi(X))) \to \mathrm{Spec}\,(R[X+a,\beta]/(\psi(X))) \\ \to \mathrm{Spec}\, H(j)^* \to 0. \end{aligned} \tag{10}$$

Over K, short exact sequence (10) appears as

$$0 \to \mathrm{Spec}\, KC_p^* \to \mathrm{Spec}\, K(C_p \times C_p)^* \to \mathrm{Spec}\, KC_p^* \to 0.$$

And so, (10) is now

$$0 \to \mathrm{Spec}\, R[\alpha] \to \mathrm{Spec}\, R[\gamma + a, \beta] \to \mathrm{Spec}\, H(j)^* \to 0 \tag{11}$$

where

$$\begin{aligned} a &= \eta(e_{0,1} + e_{1,1} + \cdots + e_{p-1,1}) + 2\eta(e_{0,2} + e_{1,2} + \cdots + e_{p-1,2}) \\ &\quad + \cdots + (p-1)\eta(e_{0,p-1} + e_{1,p-1} + \cdots + e_{p-1,p-1}), \end{aligned}$$

$$\begin{aligned} \beta &= t^j(e_{0,1} + e_{1,1} + \cdots + e_{p-1,1}) + 2t^j(e_{0,2} + e_{1,2} + \cdots + e_{p-1,2}) \\ &\quad + \cdots + (p-1)t^j(e_{0,p-1} + e_{1,p-1} + \cdots + e_{p-1,p-1}), \end{aligned}$$

$$\begin{aligned} \gamma &= t^i(e_{1,0} + e_{1,1} + \cdots + e_{1,p-1}) + 2t^i(e_{2,0} + e_{2,1} + \cdots + e_{2,p-1}) \\ &\quad + \cdots + (p-1)t^i(e_{p-1,0} + e_{p-1,1} + \cdots + e_{p-1,p-1}). \end{aligned}$$

□

Let

$$H(i,j,\mu) = R\left[\frac{(\sigma,1)-(1,1)}{t^i}, \frac{(\sigma,1)^{[-\mu]}(1,\tau)-(1,1)}{t^j}\right],$$

$$(\sigma,1)^{[-\mu]} = \sum_{m=0}^{p-1} \binom{-\mu}{m} ((\sigma,1)-(1,1))^m,$$

$\mathrm{ord}(\mu) \geq -i + (j/p)$, be the Elder order in $K(C_p \times C_p)$, given in the Introduction.

Proposition 3.8. *Let $\eta = \mu t^i$. Then $H(i,j,\mu)^* = R[\gamma + a, \beta]$.*

Proof. One shows directly that $\langle R[\gamma + a, \beta], H(i, j, \mu)\rangle \subseteq R$, thus

$$R[\gamma + a, \beta] \subseteq H(i, j, \mu)^*.$$

Moreover, $\mathrm{disc}(R[\gamma+a, \beta]/R) = \mathrm{disc}(H(i, j, \mu)^*/R)$, hence $H(i, j, \mu)^* = R[\gamma + a, \beta]$.

□

Proposition 3.9. *Let H be an arbitrary R-Hopf order in $K(C_p \times C_p)$ that induces the short exact sequence*

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

Then H is an Elder order in $K(C_p \times C_p)$.

Proof. Taking duals yields the short exact sequence

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

and applying $\mathrm{Spec}\,-$ gives the short exact sequence

$$0 \to \mathrm{Spec}\, H(i)^* \to \mathrm{Spec}\, H^* \to \mathrm{Spec}\, H(j)^* \to 0,$$

which is an element of $\mathrm{Ext}^1_{gt}(\mathrm{Spec}\, H(j)^*, \mathrm{Spec}\, H(i)^*)$. By Proposition 3.7, H^* is of the form $R[\gamma + a, \beta]$ for γ, β as above and

$$\begin{aligned} a &= \eta(e_{0,1} + e_{1,1} + \cdots + e_{p-1,1}) + 2\eta(e_{0,2} + e_{1,2} + \cdots + e_{p-1,2}) \\ &\quad + \cdots + (p-1)\eta(e_{0,p-1} + e_{1,p-1} + \cdots + e_{p-1,p-1}), \end{aligned}$$

for some $\eta \in K$. Since $R[\gamma + a, \beta]$ is an R-algebra, $a^p \in R[\beta] = H(j)^*$. Hence

$$\mathrm{ord}(\eta^p) = p\,\mathrm{ord}(\eta) \geq j,$$

and so $\mathrm{ord}(\eta) \geq j/p$. Let $\mu = \eta/t^i$. Then

$$\mathrm{ord}(\mu t^i) = \mathrm{ord}(\eta) \geq j/p,$$

and so, $\mathrm{ord}(\mu) \geq -i + (j/p)$. Now the Elder order $H(i, j, \mu)$ exists and $H(i, j, \mu)^* = R[\gamma + a, \beta]$. Consequently, $H(i, j, \mu)^* = H^*$, and so $H = H(i, j, \mu)$.

□

References

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

[2] G. Elder, Scaffolds, Galois module structure and Hopf orders, preprint, (2012).

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

[4] R. G. Underwood, *An Introduction to Hopf Algebras*, Springer, New York, (2011).