New York Journal of Mathematics

New York J. Math. **2** (1996) 86–102.

Hopf Galois Structures on Degree p^2 Cyclic Extensions of Local Fields

Lindsay N. Childs

To Alex Rosenberg on his 70th birthday

Abstract. Let L be a Galois extension of K, finite field extensions of $\mathbb{Q}_p$, p odd, with Galois group cyclic of order p^2. There are p distinct K-Hopf algebras A_d, $d = 0, \dots, p-1$, which act on L and make L into a Hopf Galois extension of K. We describe these actions. Let R be the valuation ring of K. We describe a collection of R-Hopf orders E_v in A_d, and find criteria on E_v for E_v to be the associated order in A_d of the valuation ring S of some L. We find criteria on an extension L/K for S to be E_v-Hopf Galois over R for some E_v, and show that if S is E_v-Hopf Galois over R for some E_v, then the associated order $\mathcal{A}_d$ of S in A_d is Hopf, and hence S is $\mathcal{A}_d$-free, for all d. Finally we parametrize the extensions L/K whose ramification numbers are $\equiv -1 \pmod{p^2}$ and determine the density of the parameters of those L/K for which the associated order of S in KG is Hopf.

Contents

1. Hopf Galois Structures on Galois Field Extensions 87
2. Hopf Orders 92
3. Hopf Galois Structures 96
References 102

Let p be an odd prime, and let K be a finite extension of $\mathbb{Q}_p$ which contains a primitive p th root of unity ζ, and with valuation ring R. Let L be a Galois extension of K with Galois group G and valuation ring S. Relative Galois module theory seeks to understand S as a module over the group ring RG, or more generally over the associated order $\mathcal{A}$ of S in KG, $\mathcal{A} = \{\alpha \in KG | \alpha S \subset S\}$. Then $\mathcal{A} = RG$ and S is RG-free of rank one if and only if L/K is tamely ramified. For wildly ramified extensions, the only general criterion available is that if the associated order $\mathcal{A}$ is a Hopf order over R in KG, then S is $\mathcal{A}$-free of rank one [Ch87]. (The converse is far from true.)

Since the work of Greither and Pareigis [GP87], one knows that L/K may be a Hopf Galois extension with respect to different Hopf Galois actions on L. In

Received November 8, 1996.

Mathematics Subject Classification. 11S15, 11R33, 16W30.

Key words and phrases. Galois module, Hopf Galois extension, associated order, wildly ramified, Hopf order.

ISSN 1076-9803/96

fact, Byott has recently shown that for a Galois extension L/K with group G, the classical Hopf Galois structure is unique if and only if the order g of G is coprime to $\phi(g)$ (Euler's function) [By96]. In case L is a cyclic Galois extension of K of order p^n, then L/K has exactly p^{n-1} distinct Hopf Galois structures [Ko96]. Thus when $n = 2$ there are p distinct Hopf algebras A_d, $d = 0, \dots, p-1$, which give a Hopf Galois structure on L/K.

The existence of different Hopf Galois structures on L/K raises the possibility that S may have different Galois module properties with respect to one structure than another. For example, in [CM94] we found that the associated order of the valuation ring of $\mathbb{Q}(2^{\frac{1}{4}})$ in one Hopf Galois structure was Hopf and the associated order in the other structure was not. N. Byott [By96b] found a cyclotomic Lubin-Tate extension of local fields which has two Hopf Galois structures: one associated order is Hopf, while the second associated order $\mathcal{B}$ is not Hopf and the valuation ring is not free over $\mathcal{B}$.

In this paper we describe as algebras the Hopf algebras A_d which make L/K Hopf Galois, and their actions on L. Following [Gr92], we construct a collection of Hopf orders E_v over R inside each A_d. We find criteria on L/K in order that S be a Hopf Galois extension of R for some E_v. This implies, by [Ch87], that E_v is the associated order of S in A_d. In contrast to the examples just described, however, it turns out that if S is Hopf Galois over R for E_v, a Hopf order in A_d for some d, then the associated order of S in A_d for every d is Hopf, in particular for $A_0 = KG$. Thus in the case of cyclic Galois extensions of degree p^2, the non-classical Hopf Galois structures on L do not "tame" the wild extension L/K better than the classical structure given by the Galois group.

We apply Greither [Gr92] to find necessary and sufficient conditions on an order E_v to be realizable: that is, to be the associated order of the valuation ring of some extension L/K: the congruence condition on v is the same as for Hopf orders in KG as found by Greither. Finally, we quantify the remark in [Gr92, Remark (c), page 63] that congruence conditions on the ramification numbers of a cyclic totally ramified extension L/K of degree p^2 are "badly insufficient" for deciding whether the valuation ring S of L is Hopf Galois over R.

The concept of Hopf Galois extension of commutative rings arose in [CS69] as a merger of M. Sweedler's work on Hopf algebras and the development of Galois theory of commutative rings by S. U. Chase, D. K. Harrison and Alex Rosenberg [CHR65].

1. Hopf Galois Structures on Galois Field Extensions

We begin by recalling the main result of Greither and Pareigis [GP87].

Greither-Pareigis. *If L is a Galois extension of K with group G, then there is a bijection between Hopf Galois structures on L/K and regular subgroups of $Perm(G)$ normalized by $\lambda(G)$.*

Here $Perm(G)$ is the group of permutations of the set G, $\lambda(G)$ is the image of G in $Perm(G)$ given by left translation, and a subgroup N of $Perm(G)$ is regular if N acts transitively, has order equal to the order of G, and the stabilizer in N of any element of G is trivial. (Any two of these last conditions implies the third.)

If N is a regular subgroup of $Perm(G)$, then the group ring LN acts on $GL := Map(G, L)$ by $a\eta(f)(\sigma) = af(\eta^{-1}(\sigma))$ for a in L, σ in G, f in GL, η in N. Thus if

e_σ is the function which sends σ to 1 and τ to 0 if $\tau \neq \sigma$ in G, and η is in N, then $\eta(e_\sigma) = e_{\eta(\sigma)}$. This yields a map

$$LN \times GL \to GL.$$

The Hopf Galois structure on L is obtained by taking the fixed rings of LN and GL under the action of G, where G acts on GL by $\sigma(ae_\tau) = \sigma(a)e_{\sigma\tau}$, and acts on LN by $\sigma(a\eta) = \sigma(a)\sigma(\eta)$: the action of σ in G on η in N is by conjugation by $\lambda(\sigma)$ in $Perm(G)$.

Let G be cyclic of order p^n. Then Kohl [Ko96] has shown that the only regular subgroups N of $Perm(G)$ normalized by $\lambda(G)$ are isomorphic to G, and hence (cf. also [By96, Lemma 1, (i)]) there are exactly p^{n-1} such N.

We restrict to the case $n = 2$. Then we have

Proposition 1.1. *The subgroups of $Perm(G)$ normalized by $\lambda(G)$ are N_d for $d = 0, 1, \ldots, p-1$, where $N_d = \langle\eta\rangle$ with $\eta(\sigma^i) = \sigma^{(i-1)(1+pd)}$.*

These groups were found by using [By96, Proposition 1], a refinement of [Ch89, Proposition 1].

Proof. Clearly η is in $Perm(G)$. One verifies by induction that for any r,

$$\eta^r(\sigma^i) = \sigma^{(i-r)+(ir-\frac{r(r+1)}{2})pd}.$$

Hence η has order p^2 and the stabilizer in N_d of any σ^i is trivial. So N_d is regular. Also, for any d, $N_d \subset Perm(G)$ is normalized by $\lambda(G)$. In fact,

$$\lambda(\sigma)\eta\lambda(\sigma^{-1}) = \eta^{1+pd}.$$

For

$$\begin{aligned}\lambda(\sigma)\eta\lambda(\sigma^{-1})(\sigma^i) &= \lambda(\sigma)\eta(\sigma^{i-1})\\ &= \lambda(\sigma)(\sigma^{(i-2)(1+pd)})\\ &= \sigma^{(i-1)+(i-2)pd},\end{aligned}$$

while

$$\begin{aligned}\eta^{1+pd}(\sigma^i) &= \sigma^{i-(1+pd)+(i-1)pd}\\ &= \sigma^{(i-1)+(i-2)pd}.\end{aligned}$$

□

Example 1.2. For $p = 3$, set $d = 1$, then η is the permutation which sends σ^i to $\sigma^{4(i-1)}$; its cycle representation is

$$(0, 5, 7, 6, 2, 4, 3, 8, 1).$$

We have an action $LN \times GL \to GL$, which we will describe below. Looking at the fixed elements under the action of G, we have, first, that

$$\begin{aligned}(GL)^G &= \left\{\sum_\tau a_\tau e_\tau : \sum a_\tau e_\tau = \sum \sigma(a_\tau)e_\tau\right\} \\ &= \left\{\sum_\tau a_\tau e_\tau : a_{\sigma\tau} = \sigma(a_\tau)\right\} \\ &= \left\{\sum_\sigma \sigma(a)e_\sigma\right\}\end{aligned}$$

This is isomorphic to L under the map sending a in L to $\sum \sigma(a)e_\sigma$.

Now identify σ in G with $\lambda(\sigma)$ in $Perm(G)$. Then,

$$LN^G = \left\{\sum a_i\eta^i : \sum a_i\eta^i = \sum \sigma(a_i)\sigma(\eta^i)\right\}$$

where $\sigma(\eta^i)$ means the element η_0 of N so that $\eta_0 = \lambda(\sigma)\eta^i\lambda(\sigma)^{-1}$ in $Perm(G)$. Now

$$\sigma(\eta) = \sigma\eta\sigma^{-1} = \eta^{1+pd}$$

as we observed above, and hence $\sigma(\eta^i) = \eta^{i(1+dp)}$, and so $\sigma^k(\eta^i) = \eta^{i(1+kdp)}$. In particular, η^p is fixed under the action of G.

Let $N^p = \langle\eta^p\rangle$ and let

$$e_s = (1/p)\sum_{i=0}^{p-1}\zeta^{-si}\eta^{pi}$$

in KN^p. The e_s for $s = 0, \ldots, p-1$ are the pairwise orthogonal idempotents of KN^p corresponding to the distinct irreducible representations of KN^p: $\eta^p e_s = \zeta^s e_s$ for all s.

For v in L, set $a_v = \sum_{s=0}^{p-1} v^s e_s$. These elements, defined by Greither [Gr92], are the elements of LN^p corresponding to the tuple $(1, v, v^2, \ldots, v^{p-1})$ under the isomorphism between LN^p and $L \times L \times \cdots \times L$ induced by $\eta^p \to (1, \zeta, \zeta^2, \ldots, \zeta^{p-1})$. Thus $a_{vw} = a_v a_w$ for all v, w in L.

Proposition 1.3. *Let $L^{\langle\sigma^p\rangle} = M = K[z]$ where z^p is in K and $\sigma(z) = \zeta z$. Let LN^G correspond to the embedding β of G into $Hol(N)$ so that $\beta(\sigma) = \eta\gamma$ where $\gamma\eta\gamma^{-1} = \eta^{1+pd}$. Then $LN^G = K[\eta^p, a_v\eta]$ where $v = z^{-d}$.*

Proof. We have that $\sigma^k(\eta) = \eta^{1+kpd}$, so $\sigma^p(\eta) = \eta^{1+p^2d} = \eta$. So σ^p fixes the elements of N, and $LN^G = MN^G$. Since G fixes η^p and

$$e_s = (1/p)\sum_{i=0}^{p-1}\zeta^{-si}\eta^{pi},$$

G fixes the idempotents e_s for all s. Hence

$$\begin{aligned}\sigma(a_{z^{-d}}\eta) &= \eta^{1+pd}\sum_{s=0}^{p-1}\sigma(z^{-ds})e_s \\ &= \eta\sum_{s=0}^{p-1}\zeta^{-ds}z^{-ds}\eta^{pd}e_s \\ &= \eta\sum_{s=0}^{p-1}\zeta^{-ds}z^{-ds}\zeta^{ds}e_s \\ &= \eta\sum_{s=0}^{p-1}z^{-ds}e_s \\ &= a_{z^{-d}}\eta.\end{aligned}$$

Thus $K[\eta^p, a_v\eta] \subset LN^G$. But by Galois descent, LN^G has rank p^2 over K, and since a_{v^p} is in $K[\eta^p]$, one easily sees that $(a_v\eta)^p$ is in $K[\eta^p]$, hence $K[\eta^p, a_v\eta]$ has rank p^2 over K, hence equality. □

We observe for later use that $K[\eta^p, a_v\eta] = K[\eta^p, a_{vc}\eta]$ for any c in K. For $a_{vc} = a_v a_c$, so $a_{vc}\eta = a_c \cdot a_v\eta$, and a_c is in $K[\eta^p]$.

Let A_d denote the K-Hopf algebra $K[\eta^p, a_v\eta]$ with $v = z^{-d}$. We examine the action of $A_d = LN^G$ on L.

Since L/K is a Galois extension with Galois group $G = C_{p^2} = \langle\sigma\rangle$ and K contains ζ, a primitive pth root of unity, we can assume that $M = L^{\langle\sigma^p\rangle} = K[z]$ with z^p in K and $\sigma(z) = \zeta z$, and $L = M[x]$ with x^p in M and $\sigma^p(x) = \zeta x$. Let $v = cz^{-d}$,with c in K and $0 \leq d \leq p-1$.

Proposition 1.4. *$A_d = K[\eta^p, a_v\eta]$ acts on $L = K[z][x]$ by*

$$\eta^p = \sigma^p$$

and for a in $K[z]$

$$(a_v\eta)(ax^m) = v^m\sigma(ax^m).$$

In particular, $A_0 = K[\eta]$ with $\eta(s) = \sigma(s)$ for s in L, the classical action by the group ring of the Galois group G.

Proof. We identify L as a subset of $GL = Map(G, L)$ via the isomorphism

$$a \to \sum_{i=0}^{p-1}\sigma^i(a)e_i$$

where $e_i = e_{\sigma^i}$. Then as we observed in the proof of Proposition 1.1,

$$\eta^r(e_i) = e_{i-r-pd(ir-\frac{r(r+1)}{2})}.$$

In particular, $\eta^{pk}(e_i) = e_{i-pk}$, so

$$\eta^p\left(\sum \sigma^i(a)e_i\right) = \sum \sigma^i(a)e_{i-p} = \sum \sigma^{i+p}(a)e_i = \sum \sigma^i(\sigma^p(a))e_i$$

which corresponds to $\sigma^p(a)$ in L.

Now for a in $K[z]$,

$$\begin{aligned}(a_v\eta)(ax^m) &= \left(\sum_{s,k} \frac{1}{p} v^s \zeta^{-ks} \eta^{kp+1}\right)(ax^m) \\ &= \sum_{s,k} \frac{1}{p} v^s \zeta^{-ks} \eta^{kp+1}\left(\sum_i \sigma^i(ax^m)e_i\right) \\ &= \sum_{i,s,k} \frac{1}{p} v^s \zeta^{-ks} \sigma^i(ax^m) e_{(i-kp-1)+pd(i-1)}.\end{aligned}$$

The subscript on e is mod p^2, so if we set

$$j = i(1+pd) - (1+kp+dp),$$

then

$$\begin{aligned} i &\equiv j(1-pd) + (1+kp) \pmod{p^2} \\ &= (j+1) + p(k-jd) \end{aligned}$$

and the sum becomes

$$= \sum_{j,s,k} \frac{1}{p} v^s \zeta^{-ks} \sigma^{(j+1)+p(k-jd)}(ax^m)e_j.$$

Since σ^p fixes a in $M = K[z]$, this is

$$\begin{aligned} &= \sum_{j,s,k} \frac{1}{p} v^s \zeta^{-ks} \sigma^{j+1}(ax^m)\zeta^{(k-jd)m} e_j \\ &= \sum_j \sum_s v^s \left(\frac{1}{p}\sum_k \zeta^{-ks+km}\right)\sigma^{j+1}(ax^m)\zeta^{-jdm}e_j. \end{aligned}$$

The sum over k is p if $s = m$ and 0 otherwise. So the sum over j and s becomes

$$= \sum_j v^m \zeta^{-jdm} \sigma^{j+1}(ax^m)e_j.$$

Now $v = cz^{-d}$, so

$$\begin{aligned}\sigma^j(v^m) &= c^m\zeta^{-jdm}(z^{-dm})\\ &= \zeta^{-jdm}v^m.\end{aligned}$$

Thus the sum

$$\begin{aligned}&= \sum_j \sigma^j(v^m)\sigma^{j+1}(ax^m)e_j\\ &= \sum_j \sigma^j(v^m\sigma(ax^m))e_j\end{aligned}$$

which corresponds to $v^m\sigma(ax^m)$ in L. That is,

$$(a_v\eta)(ax^m) = v^m\sigma(ax^m).$$

□

2. Hopf Orders

Now suppose K is a finite extension of $\mathbb{Q}_p$, with valuation ring R and parameter π. Let e be the absolute ramification index of K. Assume K contains a primitive pth root of unity ζ. Then $(\zeta - 1)R = \pi^{e'}R$ and $(p-1)e' = e$.

Let $M = K[z]$ with $z^p = b$ in R, and let T be the valuation ring of M. Then we may consider the K-Hopf algebras $A_d = K[\eta^p, a_v\eta]$, where $v = z^{-d}$, as described in Section 1. (Recall that for any c in K, $K[\eta^p, a_v\eta] = K[\eta^p, a_{vc}\eta]$). In this section we extend work of Greither [Gr92][GC96] to construct a collection of Hopf orders over R in A_d for each d with $0 \le d \le p-1$. These Hopf orders are parametrized by integers i, j with $0 \le i, j \le e'$ and a unit c in R.

For i an integer, $0 \le i \le e'$, let $i' = e' - i$.

Theorem 2.1. *Let i, j be integers with $0 < i, j \le e'$. Let $H_i = R\left[\frac{\eta^p - 1}{\pi^i}\right]$, a Hopf order in $K[\eta^p]$. For $v = z^{-d}c, c$ in R, let $y = \frac{a_v\eta - 1}{\pi^j}$. Then the R-algebra $E = H_i[y]$ is an R-Hopf order in $A_d = K[\eta^p, a_v\eta]$ and a Hopf algebra extension of H_j by H_i if and only if*

$$\zeta b^{-d}c^p \equiv 1 \pmod{\pi^{i'+pj}R}$$

and

$$b^{-d}c^p \equiv 1 \pmod{\pi^{pi'+j}R}.$$

Recall that the H_i for $0 \le i \le e'$ are all the Hopf orders in the group ring $K[\eta^p]$ by Tate-Oort [TO70]. This description of the H_i goes back to Larson [La76].

Proof. The canonical map from $K[N]$ to $K[N/N^p]$ sends η^p to 1, and sends a_v to 1 and H_i to R, so the image of E is $R[\frac{\bar{\eta}-1}{\pi^j}] = H_j$. To show that E is a Hopf algebra extension of H_j by H_i, we need to show that $E \cap K[\eta^p] = H_i$. This is equivalent to showing that the monic polynomial of degree p satisfied by y over $K[\eta^p]$ has coefficients in H_i. We follow [GC96, Section 2] and utilize [Gr92, I, section 3].

Now $a_v\eta = 1 + \pi^j y$, so

$$\begin{aligned}(a_v\eta)^p &= (1+\pi^j y)^p \\ &= 1 + \sum_{r=1}^{p-1} \binom{p}{r} \pi^{jr} y^r + \pi^{jp} y^p,\end{aligned}$$

hence

$$y^p + \pi^{-jp} \sum_{r=1}^{p-1} \binom{p}{r} \pi^{jr} y^r + \frac{1-(a_v\eta)^p}{\pi^{jp}} = 0.$$

Note that $(a_v\eta)^p = a_{v^p}\eta^p$, and $\eta^p = a_\zeta$, so $(a_v\eta)^p = a_{v^p\zeta}$. Thus y satisfies a monic polynomial with coefficients in H_i if and only if in H_i,

1) π^{jp} divides $p\pi^{jr}$ for $r = 1, \dots, p-1$;
2) π^{jp} divides $1 - a_{v^p\zeta}$.

Condition 1) is equivalent to $jp \le e + j$, or $j \le e'$.
Condition 2) is the same as

$$a_{v^p\zeta} \equiv 1 \pmod{\pi^{jp} H_i},$$

which, by [Gr92, I 3.2b], is equivalent to

$$v^p\zeta \equiv 1 \pmod{\pi^{i'+pj} R},$$

or, since $v^p = b^{-d}c^p$,

$$b^{-d}c^p\zeta \equiv 1 \pmod{\pi^{i'+pj} R}.$$

Note that if $j \le e'$ then $\frac{1-(a_v\eta)^p}{\pi^{pj}} \in E \cap K[\eta^p]$, so if $\frac{1-(a_v\eta)^p}{\pi^{pj}} \notin H_i$ then $E \cap K[\eta^p] \neq H_i$.

Now we show that E is closed under comultiplication if and only if $v^p \equiv 1 \pmod{\pi^{pi+j} R}$.

Recall that $A_d = K[\eta^p, a_v\eta]$ and T is the valuation ring of M. Let $E = R[t][y] = H_i[y]$ with $t = \frac{\eta^p - 1}{\pi^i}, y = \frac{a_v\eta - 1}{\pi^j}$. Since Δ is an algebra homomorphism, to show E is a coalgebra, it suffices to show that $\Delta(y) \in E \otimes E$.

Now $\Delta(y) \in A_d \otimes A_d = K \otimes_R (E \otimes_R E)$ and R is integrally closed. If we show that $\Delta(y) \in T \otimes_R (E \otimes_R E) = TE \otimes_T TE$, then, since E and therefore $E \otimes_R E$ are free R-modules,

$$(T \otimes_R (E \otimes_R E)) \cap (K \otimes_R (E \otimes_R E)) = E \otimes_R E,$$

and so $\Delta(y) \in E \otimes E$.

We will show, in fact, that

$$\Delta(y) \in C \otimes C$$

where $C = H_i \cdot 1 + H_i \cdot y$. Again, it is enough to show that $\Delta(y) \in TC \otimes_T TC$.

Now

$$\Delta(y) = \Delta\left(\frac{a_v\eta - 1}{\pi^j}\right) = \frac{\Delta(\alpha_v\eta) - a_v\eta\otimes a_v\eta}{\pi^j} + y\otimes(1+\pi^j y) + 1\otimes y$$

and the last two terms are in $C\otimes C$. So it suffices to show that

$$\frac{\Delta(a_v\eta) - a_v\eta\otimes a_v\eta}{\pi^j} \in TC\otimes_T TC.$$

Now a_v is a unit of TH_i. For since $v^p \in U_{pi'+j}(R)$, then $v\in U_{pi'+j}(T)$, hence by [Gr92, I 3.2(b)], $a_v \in 1+\pi^{j/p}H_i$. Since $j>0, a_v$ is a unit of TH_i. Since $a_v\eta = 1+\pi^j t \in TH_i\cdot 1 + TH_i\cdot t = TC$, therefore $\eta\in TC$. So

$$\left(\frac{\Delta(a_v) - a_v\otimes a_v}{\pi^j}\right)(\eta\otimes\eta) \in TC\otimes_T TC$$

if and only if

$$\frac{\Delta(a_v) - a_v\otimes a_v}{\pi^j} \in TH_i\otimes_T TH_i.$$

To decide if

$$\frac{\Delta(a_v) - a_v\otimes a_v}{\pi^j} \in TH_i\otimes_T TH_i$$

we identify elements of $M[\eta^p]\otimes_M M[\eta^p]$ as $p\times p$ matrices as in [Gr92, I, Section 3].

We have

$$\frac{\Delta(a_v) - a_v\otimes a_v}{\pi^j} = \frac{1}{\pi^j}\sum_{s=0}^{p-1}\left[\Delta(v^s e_s) - \sum_{0\le r,t<p,\, r+t\equiv s \pmod p} v^r e_r\otimes v^t e_t\right] = \sum_{s=1}^{p-1} v^s \sum_{r+t\ge p,\, r+t\equiv s \pmod p}\left[\frac{1-v^p}{\pi^j} e_r\otimes e_t\right].$$

Let $\frac{1-v^p}{\pi^j} = w$. Then

$$\frac{\Delta(a_v) - a_v\otimes a_v}{\pi^j}$$

corresponds to the matrix $M = \{M_{a,b}\}$ where $M_{a,b}$ is the coefficient of $e_a\otimes e_b$. Here, $M_{a,b} = 0$ if $a+b<p$, and $M_{a,b} = wv^s$ where $a+b = p+s$ for $a+b\ge p$.

Now $\frac{\Delta(a_v)-a_v\otimes a_v}{\pi^j} \in TH_i\otimes TH_i$ is equivalent, by [Gr92, I, Lemma 3.3] to: for all k, k^* with $0\le k,k^* < p$, $\pi^{i'(k+k^*)}$ divides

$$d^{k,k^*}(M) = \sum_{a=0}^{k}\sum_{b=0}^{k^*}\binom{k}{a}\binom{k^*}{b}(-1)^{a+b}M_{a,b} = \sum_{s=0}^{l}\sum_{a+b=p+s}\binom{k}{a}\binom{k^*}{b}(-1)^{a+b}M_{a,b}$$

where $k + k^* = p + l$. Since $M_{a,b} = wv^s$ for $a + b = p + s$, this is

$$= w \sum_{s=0}^{l} \sum_{a+b=p+s} \binom{k}{a}\binom{k^*}{b}(-1)^{p+s}v^s$$
$$= w \sum_{s=0}^{l} \binom{k+k^*}{p+s}(-1)^{p+s}v^s.$$

Now since $s < p$,

$$\binom{k+k^*}{p+s} = \binom{p+l}{p+s} \equiv \binom{l}{s} \pmod{p},$$

so

$$\equiv w \sum_{s=0}^{l} \binom{l}{s}(-1)^{p+s}v^s \pmod{p}$$
$$\equiv -w(1-v)^l \pmod{p}.$$

Thus $M \in TH_i \otimes TH_i$ if and only if $\pi^{i'(k+k^*)} = \pi^{i'(p+l)}$ divides $w(1-v)^l$ for all $l \geq 0$.

For $l = 0$ the condition is: $\pi^{i'p}$ divides $w = \frac{1-v^p}{\pi^j}$, or $v^p \equiv 1 \pmod{\pi^{pi'+j}}$. Assuming $v^p \equiv 1 \pmod{\pi^{pi'+j}}$, then, since $v \in U_{pi'+j}(T)$,

$$v - 1 \in \pi^{i'+\frac{j}{p}}T$$

(recall: π is the parameter for R), so

$$(v-1)^l \in \pi^{i'l+\frac{jl}{p}}T.$$

Also $w \in \pi^{pi'}R$, so

$$w(1-v)^l \in \pi^{pi'+i'l+\frac{jl}{p}}T.$$

Since $i'(k+k^*) = pi' + i'l$, therefore $\pi^{i'(k+k^*)}$ divides $d^{k+k^*}(M)$ for all k, k^*.

Thus

$$\frac{\Delta(a_v) - a_v \otimes a_v}{\pi^j} \in TH_i \otimes TH_i$$

if and only if $v^p \equiv 1 \pmod{\pi^{pi'+j}}$. That completes the proof. □

Suppose i, j satisfy $0 < i, j \leq e'$ and consider the two conditions

$$v^p \equiv 1 \pmod{\pi^{pi'+j}};$$
$$\zeta v^p \equiv 1 \pmod{\pi^{i'+pj}}.$$

Since

$$\zeta v^p - 1 = \zeta v^p - v^p + v^p - 1$$
$$= (\zeta - 1)v^p + (v^p - 1)$$

we must have two of $ord_R(\zeta v^p - 1)$, $ord_R(v^p - 1)$ and e' equal, and both $\leq$ the third (isosceles triangle inequality). For E to be a Hopf algebra and a free H_i-module requires

$$ord_R(\zeta v^p - 1) \geq i' + pj$$

and

$$ord_R(v^p - 1) \geq pi' + j.$$

Thus $i' + pj \leq e'$ or $pi' + j \leq e'$. The first is equivalent to $i \geq pj$; the second to $j' \geq pi'$. Hence:

Corollary 2.2. *In order that E be a Hopf algebra, i and j must satisfy:* $0 < i, j \leq e'$ *and* $i \geq pj$ *or* $j' \geq pi'$. □

Note: $i \geq pj$ is the condition of [Gr92, I 3.6] and [Gr92, II], cf. [Un94].
If $i + j \leq e'$, then $i' + pj \leq pi' + j$, so if $ord_R(v^p - 1) \geq pi' + j$, then

$$\begin{aligned} ord_R(\zeta v^p - 1) &\geq min\{e', ord_R(v^p - 1)\} \\ &\geq min\{e', pi' + j\} \geq i' + pj. \end{aligned}$$

So we have

Corollary 2.3. *If $i, j > 0, i + j \leq e'$ and $i \geq pj$, then E is a Hopf order with $E \cap K[\eta^p] = H_i$ if and only if $ord_R(v^p - 1) \geq pi' + j$.* □

The Hopf algebras E presumably fit within the classification of [By93], but the description of the E here is rather different that that of Byott.

3. Hopf Galois Structures

Now we consider a cyclic extension L/K with Galois group $G = \langle \sigma \rangle$ of order p^2, and see when S/R is E_v-Galois for some v.

We assume throughout this section that $i, j > 0$, $0 \leq i + j \leq e'$ and $i \geq pj$. Under these hypotheses, $p(i' + j) \leq pj' + 1$. For since $pj \leq i$, we have

$$pi \geq p^2 j > 2pj - 1$$

so

$$\begin{gathered} 1 - pj > -pi + pj, \\ 1 + pe' - pj > pe' - pi + pj, \end{gathered}$$

which is

$$pj' + 1 > p(i' + j).$$

Suppose S/R is E_v-Galois. Then T/R is H_j-Galois and S/T is $T \otimes H_i$-Galois, by [Gr92]. Since $i, j > 0$, M/K and L/M are totally, hence wildly ramified.

If T/R is H_j-Galois, then (cf. [Ch87]) $M = K[z]$ with $z^p = 1 + u\pi^{pj'+1}$ and $t = \frac{z-1}{\pi^{j'}}$ is a parameter for T, so $T = R[t]$. Since $\sigma(t) = \frac{\zeta-1}{\pi^{j'}}z + t = t + ut^{pj}$ for u some unit of T, the ramification number $t_1^{G/H} = pj - 1$. The converse also holds: c.f [Ch87] or [Gr92]. By [Se62, Ch. V, Sec. 1, Cor. to Prop. 3], $t_1^{G/H} = t_1^G$, so $t_1^G = pj - 1$.

Similarly, if S/T is $T \otimes H_i$-Galois, M/K is totally ramified, and t is a parameter for T, we may find x in L so that $L = M[x]$ with $\sigma^p(x) = \zeta x$ and $x^p = \gamma = 1 + ut^{p^2 i'+1}$ for some unit u of T. Then $w = \frac{x-1}{\pi^{i'}}$ is a parameter for S, and

$$\sigma^p(w) = \frac{\zeta - 1}{\pi^{i'}}x + w = w + w^{p^2 i}u'$$

for some unit u' of S. So the ramification number for L/M is $t_1^H = p^2 i - 1$, and conversely. Since $t_1^H = t_2^G$, we have $t_2^G = p^2 i - 1$.

Now L is a Galois extension of K with group $G = \langle\sigma\rangle$, cyclic of order p^2, so $\sigma(x) = \beta x$ for some β in T with $N_{M/K}(\beta) = \zeta$. If $ord_T(x^p - 1) = p^2 i' + 1$, then $\sigma(w) = \frac{\beta-1}{\pi^{i'}}x + w$, so since $t_1^G = pj - 1$, $ord_L(\frac{\beta-1}{\pi^{i'}}) = pj$. Thus

$$ord_L(\beta - 1) = p^2 i' + pj$$

and so

$$ord_M(\beta^p - 1) = p^2 i' + pj.$$

Lemma 3.1. *β is unique modulo $t^{pi'+pj}T$.*

Proof. Let $\gamma = x^p = 1 + ut^{p^2 i'+1}$ for some unit u of T.

Suppose we replace x by $x\alpha$ for some $\alpha \in T$. Then

$$(x\alpha)^p = \gamma\alpha^p = (1 + ut^{p^2 i'+1})\alpha^p.$$

If $ord_T((x\alpha)^p - 1) = p^2 i' + 1$, then $ord_T(\alpha^p - 1) \geq p^2 i' + 1$. If $ord_T(\alpha - 1) = s$, then $ord_T(\alpha^p - 1) = ps$ unless $pe' \leq s$. Assuming $s \leq pe'$, then we require

$$ps \geq p^2 i' + 1,$$

so

$$s \geq pi' + 1.$$

Now if we replace x by $x\alpha$, then $\sigma(x\alpha) = \beta\frac{\sigma(\alpha)}{\alpha}(x\alpha)$, so β is replaced by $\beta\frac{\sigma(\alpha)}{\alpha}$. If $ord_T(\alpha - 1) = s$ then by [Wy69, Theorem 22],

$$\begin{aligned} ord_T\left(\frac{\sigma(\alpha)}{\alpha} - 1\right) &\geq s + pj - 1 \\ &\geq pi' + 1 + pj - 1 = p(i' + j). \end{aligned}$$

So $\beta\frac{\sigma(\alpha)}{\alpha} \equiv \beta \pmod{t^{p(i'+j)}T}$.

Thus β is unique modulo $t^{p(i'+j)}T$. □

Given L/K with ramification numbers $t_1^G = pj-1$ and $t_2^G = p^2i-1$, when is there some E_v so that S/R is E_v-Galois? Since the discriminant over R of S equals the discriminant of the dual of E_v, S will be E_v-Galois if and only if E_v acts on S (see [Gr92, II, Section 1]), that is, $\xi \cdot s$ is in S (not just in L) for all $\xi \in E_v$ and $s \in S$. Equivalently, $E_v \subset \mathcal{A}$, the associated order of S in A_d.

We know $\mathcal{A}$ is an algebra. So to show $E_v \subset \mathcal{A}$ it suffices to show that

$$t = \frac{\eta^p - 1}{\pi^i} \in \mathcal{A}$$

and

$$y = \frac{a_v\eta - 1}{\pi^j} \in \mathcal{A}.$$

Now

$$\begin{aligned}\Delta(t) &= \frac{\eta^p \otimes \eta^p - 1 \otimes 1}{\pi^i} \\ &= \left(\frac{\eta^p - 1}{\pi^i}\right) \otimes \eta^p + 1 \otimes \left(\frac{\eta^p - 1}{\pi^i}\right) \\ &= t \otimes (1 + \pi^i t) + 1 \otimes t.\end{aligned}$$

Hence if

$$t\left(\frac{z-1}{\pi^{j'}}\right) \in S,$$

then since L is an A_d-module algebra,

$$t\left(R\left[\frac{z-1}{\pi^{j'}}\right]\right) \subset S,$$

so $tT \subset S$. Also, if

$$t\left(\frac{x-1}{\pi^{i'}}\right) \in S$$

then

$$t\left(T\left[\frac{x-1}{\pi^{i'}}\right]\right) \subset S,$$

so $tS \subset S$ and $t \in \mathcal{A}$. Hence $H_i \subset \mathcal{A}$.

Similarly, we showed in the proof of Theorem 2.1 that $C = H_i \cdot 1 + H_i \cdot y$ is a subcoalgebra of E_v. If

$$y\left(\frac{z-1}{\pi^{j'}}\right) \in S$$

then

$$C\left(\frac{z-1}{\pi^{j'}}\right) \subset S,$$

so $CT \subset S$. Also, if

$$y\left(\frac{x-1}{\pi^{i'}}\right) \in S$$

then

$$C\left(\frac{x-1}{\pi^{i'}}\right) \subset S,$$

so, since

$$S = R\left[\frac{z-1}{\pi^{j'}}\right]\left[\frac{x-1}{\pi^{i'}}\right],$$

$CS \subset S$. So $C \subset \mathcal{A}$. Since C generates E_v as an R-algebra, $E_v \subset \mathcal{A}$.

Thus E_v acts on S if and only if $t = \frac{\eta^p - 1}{\pi^i}$ and $y = \frac{a_v\eta - 1}{\pi^j}$ map $\frac{z-1}{\pi^{j'}}$ and $\frac{x-1}{\pi^{i'}}$ into S.

We see that

$$t\left(\frac{z-1}{\pi^{j'}}\right) = 0,$$

$$y\left(\frac{z-1}{\pi^{j'}}\right) = \frac{\sigma^{-1}(z) - z}{\pi^{e'}} = \frac{\zeta^{-1} - 1}{\pi^{e'}} z \in T,$$

and

$$t\left(\frac{x-1}{\pi^{i'}}\right) = \frac{\zeta^{-1} - 1}{\pi^{e'}} x \in S;$$

finally, by Proposition 1.4,

$$y\left(\frac{x-1}{\pi^{i'}}\right) = \frac{a_v\eta(x) - x}{\pi^{i'+j}} = \frac{v\sigma(x) - x}{\pi^{i'+j}} = \frac{v\beta - 1}{\pi^{i'+j}} x$$

is in S if and only if

$$\beta \equiv v^{-1} \pmod{\pi^{i'+j}T}.$$

From this we have

Proposition 3.2. *Let L/K be a Galois extension with group G cyclic of order p^2 and with ramification numbers $t_1 = pj - 1$ and $t_2 = p^2 i - 1$, where i, j satisfy the inequalities at the beginning of this section. Then the valuation ring S of L is E_v-Hopf Galois over R, and hence the associated order of S in A_d is Hopf, if and only if $\beta \equiv v^{-1} \pmod{\pi^{i'+j}T}$.* □

Now we observe

Lemma 3.3. *If $v \equiv z^{-d}c$ for some c in R, then $v \equiv c \pmod{\pi^{i'+j}T}$.*

Proof. We have

$$z = 1 + ut^{pj'+1},$$

u a unit of T. Since $pj' + 1 > p(i' + j)$,

$$z \equiv 1 \pmod{\pi^{i'+j}T = t^{p(i'+j)}T}.$$

□

Corollary 3.4. *With the hypotheses of Proposition 3.2, if S is E_v-Galois then p divides j.*

Proof. We have $ord_T(\beta-1) = pi'+j$, and so $ord_T(v^{-1}-1) = ord_T(v-1) = pi'+j$. Hence $ord_R(v^p - 1) = pi' + j$.

Since $v = z^{-d}c$ and $pi' + j < pj' + 1$, we have

$$ord_R(v^p - 1) = pi' + j < pj' + 1 = ord_R(z^p - 1),$$

so $ord_R(v^p - 1) = ord_R(c^p - 1) = p\; ord_R(c - 1)$. Hence $ord_R(c - 1) = i' + j/p$, and p divides j. □

Corollary 3.5. *With the hypotheses of Proposition 3.2, if S/R is Hopf Galois for some E_v, then S is free over the associated order in A_d for all d.*

Proof. We have that S/R is Hopf Galois for E_v, $v = z^{-d}c$, if and only if

$$\beta \equiv (z^{-d}c)^{-1} \pmod{\pi^{i'+j}T}.$$

But

$$z^{-d} \equiv 1 \pmod{\pi^{i'+j}T},$$

and hence

$$\beta \equiv (z^{-d}c)^{-1} \pmod{\pi^{i'+j}T}$$

for every d, and so E_v acts on S when $v = z^{-d}c$ for every d. Hence for any d, S/R is $E_{z^{-d}c}$-Hopf Galois, and so $E_{z^{-d}c}$ is the associated order of S in A_d for every d. □

Corollary 3.6. *E_v is realizable if and only if $ord_T(v - 1) = pi' + j$.*

Proof. If L/K realizes E_v, that is, E_v is the associated order of the valuation ring of the Galois extension L of K, then, as we showed, $\beta \equiv v^{-1} \pmod{\pi^{i'+j}T}$, so $ord_T(v - 1) = pi' + j$. Conversely, if $ord_T(v - 1) = pi' + j$, then since $v = cz^{-d}$ for some $c \in R$, $ord_T(c - 1) = pi' + j$, so E_c is realizable by some L/K by [Gr92, Part II, Section 3]. But then, since $cz^{-d} \equiv c \pmod{\pi^{i'+j}T}$, we see that the extension L/K also realizes E_v by Proposition 3.2. □

The problem raised at the beginning of this section can be precisely answered by the following corollary, in which the hypotheses on L are recapitulated.

Corollary 3.7. *Let K be a finite extension of $\mathbb{Q}_p$ containing ζ_p, a primitive pth root of unity. Let L be a cyclic Galois extension of K with Galois group $G = \langle\sigma\rangle$ of degree p^2 with intermediate field M and with ramification numbers $t_1^G = pj - 1$ and $t_2^G = p^2 i - 1$ where $0 < pj \le i, p$ divides j, and $i + j \le e' = e_{K/\mathbb{Q}_p}/(p-1)$. Let S, T and R be the valuation rings of L, M and K, respectively. Let $L = M[x]$ with $ord_M(x^p - 1) = p^2 i' + 1$ and $\sigma(x) = \beta x$. Then S is an E_v-Hopf Galois extension of R if and only if β is congruent to an element of R modulo $t^{pi'+pj}T = \pi^{i'+j}T$.*

Proof. The ramification conditions on L/K are equivalent to T/R being H_j- Hopf Galois and S/T being $T \otimes H_i$-Hopf Galois. Then S is E_v-Hopf Galois for some v if and only if $\beta \equiv v^{-1} \pmod{t^{p(i'+j)}T}$ by Proposition 3.2, and

$$v \equiv c \pmod{\pi^{i'+j}T}$$

with $c \in R$ by Lemma 3.3. Thus S is E_v-Hopf Galois if and only if the element β which by Lemma 3.1 is uniquely associated to L is congruent to an element of R modulo $\pi^{i'+j}T$. □

Lemma 3.1 implies that there is a well-defined map from the set of cyclic extensions L of K containing M satisfying the hypotheses of Corollary 3.7 to

$$U_{pi'+j}(T)/U_{pi'+pj}(T),$$

and hence to

$$U_{pi'+j}(T)/U_{pi'+j+p-1}(T).$$

Call that map ϕ.

Corollary 3.8. *ϕ maps onto the classes $\bar{U}$ of $U_{pi'+j}(T)/U_{pi'+j+p-1}(T)$ represented by β in T with $ord_T(\beta - 1) = pi' + j$.*

Proof. Let β be any element of T with $ord_T(\beta - 1) = pi' + j$. We first show that β may be modified by an element of $U_{pi'+j+p-1}(T)$ to an element of norm ζ.

By [Wy69, Theorem 22], the map $\sigma - 1$ yields an isomorphism

$$U_{pi'+j+r-(pj-1)}(T)/U_{pi'+j+r+1-(pj-1)}(T) \to U_{pi'+j+r}(T)/U_{pi'+j+r+1}(T)$$

for all r such that $pi' + j + r - pj + 1$ is not divisible by p. Since p divides j, we obtain such an isomorphism for $r = 0, 1, \ldots, p-2$. Thus any β_r in $U_{pi'+j+r}(T)$ is of the form $\beta_r = \frac{\sigma(\alpha_r)}{\alpha_r}\beta_{r+1}$ for some $\beta_{r+1} \in U_{pi'+j+r+1}(T)$. Making that observation for $r = 0, 1, \ldots, p-2$, we see that any β_0 with $ord_T(\beta_0 - 1) = pi' + j$ may be written as $\beta_0 = \frac{\sigma(\alpha)}{\alpha}\beta_{p-1}$ for some α in $U(T)$ and some β_{p-1} in $U_{pi'+j+p-1}(T)$. Thus every β in T with $ord_T(\beta - 1) = pi' + j$ may be multiplied by an element of $U_{pi'+j+p-1}(T)$ to obtain an element β' of norm 1. That is, the class of any β_0 in $U_{pi'+j}(T)/U_{pi'+j+p-1}(T)$ contains an element of norm 1.

By [Gr92, Lemma 3.8], there exists an element $\delta \in U_{pi'+pj}(T)$ of norm ζ. Multiplying the representative in the class of β_0 with norm 1 by δ gives an element β in the class of β_0 of norm ζ.

Any β with $ord_T(\beta - 1) = pi' + j$ and norm $= \zeta$ is in the image of ϕ. For by the proof of [Gr92, Lemma 3.9], we may find γ in $U(T)$ with $ord_T(\gamma - 1) = p^2 i' + 1$ and $\frac{\sigma(\gamma)}{\gamma} = \beta^p$; such a γ yields a cyclic extension L/K of degree p^2 satisfying the hypotheses of Corollary 3.7 with $\sigma(x) = \beta x$.

Thus any class in $U_{pi'+j}(T)/U_{pi'+j+p-1}(T)$ represented by an element β with $ord_T(\beta) = pi' + j$ is represented by such a cyclic extension. □

Let $q = |R/\pi R|$. Then the number of elements of $U_{pi'+j}(T)/U_{pi'+j+p-1}(T)$ of order $pi'+j$ is easily seen to be $(q-1)q^{p-2}$ (expand elements of $U_{pi'+j}(T)$ t-adically).

Only $q-1$ of these have classes represented by units of R. Thus the field extensions L/K satisfying the hypotheses of Corollary 3.7 map by ϕ onto $\bar{U}$, but those whose valuation rings S are Hopf Galois over R map onto a subset of $\bar{U}$ of density $\frac{1}{q^{p-2}}$. This may illuminate Greither's remark [Gr92, Remark (c), p. 63] that congruence conditions on the ramification numbers are badly insufficient for insuring that S/R is Hopf Galois.

References

[By93] N. P. Byott, *Cleft extensions of Hopf algebras II*, Proc. London Math. Soc. **(3) 67** (1993), 277–304.

[By96] N. P. Byott, *Uniqueness of Hopf Galois structure for separable field extensions*, Comm. Algebra **24** (1996), 3217–3228, 3705.

[By96b] N. P. Byott, *Galois structure of ideals in abelian p-extensions* (to appear).

[CHR65] S. U. Chase, D. K. Harrison, A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Galois Theory and Cohomology of Commutative Rings (by S. U. Chase, D. K. Harrison and A. Rosenberg), Memoirs Amer. Math. Soc. no. 52, Springer-Verlag, Berlin, 1965, pp. 15–33.

[CS69] S. U. Chase, M. Sweedler, *Hopf Algebras and Galois Theory*, Lecture Notes in Mathematics No. 97, Springer-Verlag, Berlin, 1969.

[Ch87] L. N. Childs, *Taming wild extensions with Hopf algebras*, Trans. Amer. Math. Soc. **304** (1987), 111–140.

[Ch89] L. N. Childs, *On the Hopf Galois theory for separable field extensions*, Comm. Algebra **17** (1989), 809–825.

[CM94] L. N. Childs, D. J. Moss, *Hopf algebras and local Galois module theory*, Advances in Hopf Algebras (J. Bergen, S. Montgomery, eds), Marcel Dekker, New York, 1994, pp. 1–24.

[Gr92] C. Greither, *Extensions of finite group schemes, and Hopf Galois theory over a discrete valuation ring*, Math. Zeitschrift **220** (1992), 37–67.

[GC96] C. Greither, L. Childs, *p-elementary group schemes - constructions, and Raynaud's theory* (to appear).

[GP87] C. Greither, B. Pareigis, *Hopf Galois theory for separable field extensions*, J. Algebra **106** (1987), 239–258.

[Ko96] Timothy Kohl, *Classification of the Hopf Galois structures on prime power radical extensions* (to appear).

[La76] R. G. Larson, *Hopf algebras defined by group valuations*, J. Algebra **38** (1976), 414–452.

[Se62] J.-P. Serre, *Corps Locaux*, Hermann, Paris, 1962.

[TO70] J. Tate, F. Oort, *Group schemes of prime order*, Ann. Scient. Ec. Norm. Sup. **3** (1970), 1–21.

[Un94] R. G. Underwood, *R-Hopf algebra orders in KC_{p^2}*, J. Algebra **169** (1994), 418–440.

[Wa95] W. C. Waterhouse, *The normal closures of certain Kummer extensions*, Canad. Math. Bull. **37** (1994), 133–139.

[Wy69] B. F. Wyman, *Wildly ramified Gamma extensions*, Amer. J. Math. **91** (1969), 135–152.

Department of Mathematics and Statistics, University at Albany, Albany, NY 12222
lc802@math.albany.edu

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX