New York Journal of Mathematics

New York J. Math. **17** (2011) 51–74.

Hopf Galois structures on Kummer extensions of prime power degree

Lindsay N. Childs

Abstract. Let K be a field of characteristic not p (an odd prime), containing a primitive p^n-th root of unity ζ, and let $L = K[z]$ with $x^{p^n} - a$ the minimal polynomial of z over K: thus $L|K$ is a Kummer extension, with cyclic Galois group $G = \langle\sigma\rangle$ acting on L via $\sigma(z) = \zeta z$. T. Kohl, 1998, showed that $L|K$ has p^{n-1} Hopf Galois structures. In this paper we describe these Hopf Galois structures.

Contents

1. Introduction

Chase and Sweedler [CS69] introduced the concept of a Hopf Galois extension, generalizing the notion of a classical Galois extension of fields $L|K$ with Galois group G. Given a field extension $L \supset K$ and a cocommutative K-Hopf algebra H that acts on L making L into an H-module algebra (i.e., $h(ab) = \sum_{(h)} h_{(1)}(a)h_{(2)}(b)$, where, following Sweedler's notation, the comultiplication $\Delta : H \to H \otimes_K H$ is given on an element h of H by

$$\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)},$$

then L is an H-Hopf Galois extension of K if the obvious map

$$L \otimes_K H \to \mathrm{End}_K(L)$$

induced from the module action of H on L is 1-1 and onto.

Received January 31, 2010.
2000 *Mathematics Subject Classification.* 12F10.
Key words and phrases. Hopf Galois extension, Kummer extension, p-adic logarithm.

ISSN 1076-9803/2011

If L is a Galois extension of K with Galois group G, then L is a KG-Hopf Galois extension of K.

For some time after the concept was introduced, there was little interest in applying it to classical Galois extensions of fields, until in [GP87], Greither and Pareigis showed that a classical Galois extension $L|K$ of fields with Galois group G could have Hopf Galois structures other than the classical one by KG, and showed how to transform the problem of determining the number of Hopf Galois structures on $L|K$ into one depending purely on the Galois group G.

Subsequently, Byott [By96], extending [Ch89], found a translation of the group-theoretic problem that made the problem of counting Hopf Galois structures on $L|K$ far more tractable. Thus most of the results on Hopf Galois structures on field extensions with given Galois group G have utilized Byott's translation, in particular, [By96], [Ko98], [CaC99], [By02], [Ch03], [By04a], [By04b], [Ch05], [By07], [Ch07], [CCo07], [FCC11]. Other than the original paper of Greither and Pareigis [GP87] very few papers explicitly use the direct approach of [GP87] to determine Hopf Galois structures and even fewer explicitly describe the K-Hopf algebra and the action of the Hopf algebra on the field extension L. The most notable exceptions are papers that utilize the Kummer theory of formal groups to yield Hopf Galois structures (see [Ch00], Chapter 12), results where the Galois group has order p^2, p an odd prime (see [Ch96] and [By02]), and work of Kohl [Ko07], for groups G of order $4p$, p an odd prime.

For Galois extensions $L|K$ of local number fields with Galois group G, a classical problem in local Galois module theory is to understand the valuation ring S of L as a module over the group ring RG, where R is the valuation ring of K. E. Noether showed that S is a free RG-module if and only if $L|K$ is tamely ramified. In the wild (= non-tame) case Leopoldt showed that sometimes S is a free $\mathfrak{A}$ module where $\mathfrak{A}$ is the associated order of S in KG. More generally, if $L|K$ is an H-Hopf Galois extension and $\mathfrak{A}$, the associated order of S in H, is an R-Hopf order in H, then S is $\mathfrak{A}$-free [CM94]. Byott ([By97a], [By97b], [By99], [By00], [By02]) has constructed examples of wild Galois extensions $L|K$ of local fields with Galois group G where S is not a free module over the associated order in KG, but the associated order in some other H-Hopf Galois structure on $L|K$ is an R-Hopf order in H, and hence S is free over that associated order . Thus the existence of Hopf Galois structures other than the classical one for Galois extensions of local fields adds an array of new possibilities for the study of local Galois module structure.

The purpose of this paper is to study the Hopf Galois structures on a cyclic extension $L|K$ of order p^n, where p is an odd prime. It has been known since [Ko98] that there are p^{n-1} Hopf Galois structures on $L|K$, but except for $n \leq 2$ the K-Hopf Galois structures have not been described. In this paper, when L is a cyclic Kummer extension of K of degree p^n, p an

odd prime, we describe the K-Hopf algebras H as K-algebras for each of the p^{n-1} Hopf Galois structures, and describe how the elements of H act on L.

Acknowledgements. My thanks to the Mathematics Department at Virginia Commonwealth University for its hospitality while this research was conducted, and to a referee for numerous helpful comments on a previous version of this paper.

2. Greither–Pareigis theory and Byott's translation

In order to pass from results obtained via Byott's translation to a more explicit description of the Hopf Galois structures, we need to examine the Greither–Pareigis and Byott results in some detail.

Let $L|K$ be a Galois extension with Galois group G. Then the map

$$\gamma : L \otimes_K L \to \mathrm{Hom}_L(LG, L) := GL$$

by $\gamma(a \otimes b)(\sigma) = a\sigma(b)$ is an isomorphism. If $\{x_\sigma : \sigma \in G\}$ is the dual basis of $\{\sigma \in G\}$, then $L \cong K \otimes_K L$ maps under γ into GL and the image $\gamma(1 \otimes b)$ satisfies

$$\gamma(1 \otimes b)(\sigma) = \sigma(b)$$

for all σ in G. Thus

$$\gamma(1 \otimes b) = \sum_{\sigma \in G} \sigma(b) x_\sigma,$$

and for τ in G,

$$\begin{aligned} \gamma(1 \otimes \tau(b)) &= \sum_{\sigma \in G} \sigma(\tau(b)) x_\sigma \\ &= \sum_{\sigma \in G} \sigma(b) x_{\sigma\tau^{-1}} \\ &= \sum_{\sigma \in G} \sigma(b) x_{\rho(\tau)(\sigma)} \end{aligned}$$

where $\rho : G \to \mathrm{Perm}(G)$ is the right regular representation. Thus the action of G on $L \cong K \otimes L$ corresponds under base change to an action of G on $GL = \sum_\tau L x_\tau$ making GL a Galois extension of L with Galois group G acting as permutations of the dual basis $\{x_\sigma\}$ via ρ.

A subgroup N of $\mathrm{Perm}(G)$ is regular if N has the same order as G and the orbit in G of each element of G under action by N is all of G.

Greither and Pareigis showed that given any Hopf Galois structure on $L|K$ by a K-Hopf algebra H, then $L \otimes_K H = LN$ for some regular subgroup N of $\mathrm{Perm}(G)$ acting on GL by permuting the (subscripts of the) dual basis $\{x_\sigma\}$. Also, N is normalized by $\lambda(G)$, the image in $\mathrm{Perm}(G)$ of G under the left regular representation λ of G, $\lambda(\sigma)(\tau) = \sigma\tau$. Conversely, each regular subgroup N of $\mathrm{Perm}(G)$ defines an LN-Hopf Galois structure on GL by permuting the dual basis $\{x_\sigma\}$, and if N is normalized by $\lambda(G)$, then

that Hopf Galois structure descends to an $(LN)^G$-Hopf Galois structure on $(GL)^G \cong L$, where G acts on GL by

$$\tau(ax_\sigma) = \tau(a)x_{\lambda(\tau)(\sigma)}$$

for τ, σ in G, a in L, and G acts on LN by

$$\tau(a\eta) = \tau(a)\lambda(\tau)\eta\lambda(\tau)^{-1}$$

for τ in G, η in N and a in L. Thus there is a bijection between Hopf Galois structures on $L|K$ and regular subgroups of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$.

Byott's translation works as follows. Given a Galois extension $L|K$ with Galois group G, let N be a group with the same cardinality as G. Inside $\mathrm{Perm}(N)$ is $\mathrm{Hol}(N)$, the normalizer of $\lambda(N)$. Then $\mathrm{Hol}(N) = \rho(N)\cdot\mathrm{Aut}(N)$. Each homomorphism $\beta : G \to \mathrm{Hol}(N)$ so that $\beta(G)$ is a regular subgroup of $\mathrm{Perm}(N)$ yields a Hopf Galois structure on $L|K$, as follows: Given β, define the function $b : G \to N$ by $b(\sigma) = \beta(\sigma)(e)$, where e is the identity element of N. Since $\beta(G)$ is a regular subgroup of $\mathrm{Perm}(N)$, b is a bijection. Then b defines an isomorphism between $\mathrm{Perm}(N)$ and $\mathrm{Perm}(G)$ by the map that sends π in $\mathrm{Perm}(N)$ to $C(b^{-1})(\pi) = b^{-1}\pi b$ in $\mathrm{Perm}(G)$. So define an embedding $\alpha : N \to \mathrm{Perm}(G)$ by

$$\alpha(\eta)(\sigma) = b^{-1}(\lambda(\eta)(b(\sigma)))$$

for σ in G, η in N. As Byott [By96] showed, two regular embeddings $\beta, \beta' : G \to \mathrm{Perm}(N)$ define the same regular subgroup $\alpha(N)$ of $\mathrm{Perm}(G)$, hence the same Galois structure on $L|K$, iff there exists an automorphism γ of N so that $\beta'(\sigma) = C(\gamma)(\beta(\sigma)) = \gamma\beta(\sigma)\gamma^{-1}$ for all σ in G.

This translation of the problem of finding regular subgroups of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$ has made the problem of determining Hopf Galois structures on $L|K$ somewhat easier by first, splitting the problem into a number of separate problems, one for each isomorphism class of groups N of the same cardinality as G, and second, replacing the problem of finding regular subgroups of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$ by finding regular embeddings of G into $\mathrm{Hol}(N)$, typically a much smaller group. As a result, most of the results on Hopf Galois structures on field extensions with given Galois group G have utilized Byott's translation, as noted above.

Moving from results using the Byott translation to explicitly describing the Hopf Galois structure involves two obstacles: first, using the function b (rarely a homomorphism) to translate from a regular embedding $\beta : G \to \mathrm{Hol}(N)$ to the corresponding embedding $\alpha : N \to \mathrm{Perm}(G)$, and secondly, descending the action of $\alpha(N)$ on GL to an action of $L(\alpha(N))^{\lambda(G)}$ on L.

3. The action of LN^G on L

Let $L|K$ be a Galois extension of fields with Galois group G of order n, let N be a group of order n and suppose $\beta : G \to \mathrm{Hol}(N) \subset \mathrm{Perm}(N)$ is a regular embedding. Then N gives rise to a Hopf Galois structure on $L|K$ by the K-Hopf algebra $H = LN^G \cong L\alpha(N)^{\lambda(G)}$. We describe this action.

Proposition 1. *Let $L|K$, G, N, β, H be as above. Then H acts on L as follows. For $\xi = \sum_{\eta\in N} s_\eta\eta$ in H, s_η in L and a in L,*

$$\xi(a) = \sum_{\eta} s_\eta b^{-1}(\eta^{-1})(a).$$

Proof. The regular embedding $\beta : G \to \mathrm{Hol}(N)$ yields the regular embedding $\alpha : N \to \mathrm{Perm}(G)$ via

$$\alpha(\eta)(\sigma) = b^{-1}(\lambda(\eta)(b(\sigma)).$$

For a in L, the image of a in GL is $\sum_\sigma \sigma(a)x_\sigma$, and

$$\begin{aligned}\xi\left(\sum_{\sigma\in G}\sigma(a)x_\sigma\right) &= \sum_{\eta} s_\eta\eta\left(\sum_{\sigma}\sigma(a)x_\sigma\right)\\ &= \sum_{\eta,\sigma} s_\eta\sigma(a)x_{\alpha(\eta)(\sigma)}.\end{aligned}$$

Since H maps GL^G to itself, $\xi(\sum_\sigma \sigma(a)x_\sigma)$ has the form $\sum_\sigma \sigma(c)x_\sigma$, the image in GL of an element c of L. Thus for a in L, $\xi(a) = c$, the coefficient of x_1 in the last expression (where 1 is the identity element of G).

Now $b : G \to N$ is a bijection that maps 1 in G to the identity element e of N, since β is a homomorphism. So ,

$$1 = \alpha(\eta)(\sigma) = b^{-1}(\lambda(\eta)b(\sigma))$$

iff

$$\eta b(\sigma) = e,$$

iff

$$\sigma = b^{-1}(\eta^{-1}).$$

So the coefficient of x_1 is

$$\begin{aligned}\xi(a) &= \sum_{(\eta,\sigma),\alpha(\eta)(\sigma)=1} s_\eta\sigma(a)\\ &= \sum_{\eta\in N} s_\eta b^{-1}(\eta^{-1})(a).\end{aligned}$$

□

Once we find a set of generators of $H = LN^G$, we may use the map b^{-1} to describe the action of H on L as in Proposition 1.

4. Regular embeddings for G cyclic

Let L be a Galois extension of K with Galois group G cyclic of order p^n, p an odd prime. Kohl [Ko98] showed that if $L|K$ is H-Hopf Galois, then the K-Hopf algebra H has associated group G: that is, $L \otimes_K H \cong LG$. In other terms, if there is a regular embedding of G into $\mathrm{Hol}(N)$ for N a group of order p^n, then $N \cong G$. Thus if we wish to find Hopf Galois structures on $L|K$, it suffices to seek regular embeddings β of G into $\mathrm{Hol}(G)$.

Now $\mathrm{Hol}(G) \cong G \rtimes \mathrm{Aut}(G) \cong \mathbb{Z}/p^n\mathbb{Z} \rtimes (\mathbb{Z}/p^n\mathbb{Z})^\times$, where we view elements of $\mathrm{Hol}(G)$ as of the form (a, g) with a, g integers modulo p^n and g coprime to p. Since G embeds in $\mathrm{Perm}(G)$ by the right regular representation ρ, (a, g) acts on h in G by $(a, g)(h) = (gh - a)$, and so the multiplication on G is $(a, g)(a', g') = (a + ga', gg')$. It is routine to verify that (a, g) has order p^n iff a is coprime to p and $g \equiv 1 \pmod{p}$. Thus for $G = \langle\sigma\rangle$ the regular embeddings $\beta : G \to \mathrm{Hol}(\mathbb{Z}/p^n\mathbb{Z})$ have the form $\beta(\sigma) = (a, 1 + dp)$ for a coprime to p.

Proposition 2. *Up to equivalence, the p^{n-1} equivalence classes of regular embeddings $\beta : G \to \mathrm{Hol}(G)$ are represented by β satisfying*

$$\beta(\sigma) = (-1, 1 + dp)$$

for d modulo p^{n-1}.

Proof. Given $\beta, \beta' : G \to \mathrm{Hol}(G)$, $\beta \sim \beta'$ if $\beta' = C(\gamma)\beta$ for γ in $\mathrm{Aut}(G)$. Now $(\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathrm{Aut}(G)$ via $g \mapsto \gamma_g$, left multiplication by g. For h in $G = \mathbb{Z}/p^n\mathbb{Z}$ and $\beta(\sigma) = (a, 1+dp)$ in $\mathrm{Hol}(G) = \rho(G)\cdot\mathrm{Aut}(G) \cong G \rtimes \mathrm{Aut}(G)$,

$$\begin{aligned}
\gamma_g\beta(\sigma)\gamma_g^{-1}(h) &= \gamma_g(a, 1 + dp)\gamma_g^{-1}(h) \\
&= \gamma_g(a, 1 + dp)(g^{-1}h) \\
&= \gamma_g((1 + dp)g^{-1}h - a) \\
&= g((1 + dp)g^{-1}h - a) \\
&= (1 + dp)h - ga \\
&= (ga, 1 + dp)(h).
\end{aligned}$$

For each a coprime to p, there is some g so that $ga \equiv -1 \pmod{p^n}$. Since d is unaffected by γ_g, each choice of d modulo p^{n-1} yields a different equivalence class. □

For later use we note:

Lemma 3. *For g in $(\mathbb{Z}/p^n\mathbb{Z})^\times$, $(-1, g)\lambda(a)(-1, g)^{-1} = \lambda(ga)$.*

Proof.

$$(-1, g)(g^{-1}, g^{-1}) = (-1 + g(g^{-1}), gg^{-1}) = (0, 1)$$

and so for all h in G,

$$\begin{aligned}
(-1, g)\lambda(a)(-1, g)^{-1}(h) &= (-1, g)\lambda(a)(g^{-1}, g^{-1})(h) \\
&= (-1, g)\lambda(a)(g^{-1}h - g^{-1}) \\
&= (-1, g)(a + g^{-1}h - g^{-1}) \\
&= g(a + g^{-1}h - g^{-1}) + 1 \\
&= ga + h \\
&= \lambda(ga)(h).
\end{aligned}$$

□

5. Regular subgroups of Perm(G) for G cyclic

As noted earlier, given a regular embedding $\beta : G \to \mathrm{Hol}(N)$, we obtain the corresponding regular subgroup $\alpha(N)$ of $\mathrm{Perm}(G)$ by using the bijective function $b : G \to N$ defined by $b(\sigma) = \beta(\sigma)(0)$, where 0 is the identity element of N. Then b defines an isomorphism between $\mathrm{Perm}(N)$ and $\mathrm{Perm}(G)$ by the map that sends π in $\mathrm{Perm}(N)$ to $C(b^{-1})(\pi) = b^{-1}\pi b$ in $\mathrm{Perm}(G)$. For G a cyclic group (written additively), this isomorphism yields an embedding $\alpha : N \to \mathrm{Perm}(G)$ by

$$\alpha(\theta)(\sigma) = b^{-1}(\lambda(\theta)(b(\sigma))) = b^{-1}(\theta + b(\sigma))$$

for σ in G, θ in N. The subgroup of $\mathrm{Perm}(G)$ corresponding to β is then $\alpha(N)$, and the action of LN^G on L is described by b^{-1}, as in Proposition 1.

For G cyclic of order p^n, $N \cong G$ and the group $M = \alpha(G) \subset \mathrm{Perm}(G)$ is generated by $\eta = \alpha(1)$, the permutation that sends q in G to $b^{-1}(b(q) + 1)$. In particular, for $q = b^{-1}(k)$, we have

$$\eta(b^{-1}(k)) = b^{-1}(bb^{-1}(k) + 1) = b^{-1}(k + 1).$$

Thus the cycle description of the generator η of $\alpha(G)$ in $\mathrm{Perm}(G)$ is

$$(b^{-1}(1), b^{-1}(2), b^{-1}(3), \ldots).$$

To find $b^{-1} : N \to G$, we have

Proposition 4. *Let $G = \mathbb{Z}/p^n\mathbb{Z}$, p odd, and let $\beta : G \to \mathrm{Hol}(G)$ with $\beta(1) = (-1, g)$ for $g = 1 + dp$ as in Proposition 2. Then for t, s in G,*

$$\beta(t) = \left(-\frac{g^t - 1}{g - 1}, g^t\right),$$
$$b(t) = \frac{(1 + dp)^t - 1}{dp}$$
$$b^{-1}(s) = \frac{\log_p(1 + sdp)}{\log_p(1 + sp)}$$

where $\log_p(y)$ is the p-adic logarithm function.

Proof. If $\beta : G \to \mathrm{Hol}(G)$ with $\beta(1) = (-1, g)$ for $g = 1 + dp$, then

$$\beta(t) = (-1, g)^t = (-(1 + g + g^2 + \ldots + g^{t-1}), g^t) = \left(-\left(\frac{g^t - 1}{g - 1}\right), g^t\right).$$

so

$$b(t) = \beta(t)(0) = (-1, g)^t(0).$$

For $g = 1 + dp$,

$$\begin{aligned}(-1, g)^t &= \left(\frac{-\sum_{r=1}^{t} \binom{t}{r} (dp)^r}{dp}, \sum_{r=0}^{t} \binom{t}{r} (dp)^r \right) \\ &= \left(-\sum_{r=1}^{t} \binom{t}{r} (dp)^{r-1}, \sum_{r=0}^{t} \binom{t}{r} (dp)^r \right), \\ &= \left(-\frac{(1+dp)^t - 1}{dp}, \sum_{r=0}^{t} \binom{t}{r} (dp)^r \right).\end{aligned}$$

So

$$s = b(t) = \beta(t)(0) = \frac{(1+dp)^t - 1}{dp}.$$

Thus $t = b^{-1}(s)$ where

$$1 + sdp = (1 + dp)^t.$$

Solving for t is the same as solving the discrete logarithm problem in the cyclic group $(1 + p\mathbb{Z})/(1 + p^n\mathbb{Z})$.

For x a multiple of p, the p-adic logarithm function is

$$\log_p(1 + x) = \sum_{i=1}^{\infty} (-1)^{i-1} \frac{x^i}{i}.$$

For x, y both multiples of p, $\log_p((1 + x)(1 + y)) = \log_p(1 + x) + \log_p(1 + y)$, and $\log_p : (1 + p\mathbb{Z})/(1 + p^n\mathbb{Z}) \to p\mathbb{Z}/p^n\mathbb{Z}$ is bijective [Co00, 4.2.7, 4.2.8]. Thus from $1 + sdp = (1 + dp)^t$ we obtain

$$\log_p(1 + sdp) = \log_p((1 + dp)^t) = t \log_p(1 + dp)$$

and so

$$t = b^{-1}(s) = \frac{\log_p(1 + sdp)}{\log_p(1 + dp)}.$$ □

Example 5. Let $p = 3$, $G = \mathbb{Z}/9\mathbb{Z}$ and $d = 1$, so $g = 4$. Then for $t \geq 0$,

$$\beta(t) = (-1, 4)^t,$$

so

$$\begin{aligned}b(t) &= \frac{(1+p)^t - 1}{p} = t + \frac{t(t-1)}{2} p + \dots \\ &\equiv t + 6t(t-1) \pmod 9.\end{aligned}$$

Thus

$$\begin{aligned}b(3r) &= 3r \\ b(1 + 3r) &= 1 + 3r \\ b(2 + 3r) &= (2 + 3r) + 3,\end{aligned}$$

hence

$$b^{-1}(3r) = 3r$$
$$b^{-1}(1+3r) = 1+3r$$
$$b^{-1}(2+3r) = (2+3r)-3.$$

As an element of Perm(G), the generator η of $\alpha(G)$ has cycle description

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

Since $\lambda(1) = (0,1,2,3,4,5,6,7,8)$, one may verify easily that

$$\lambda(1)\eta\lambda(1)^{-1} = \eta^4.$$

6. Determining the K-Hopf algebra

For the remainder of the paper we assume that K contains a primitive p^n-th root of unity ζ, p odd, and L is a Kummer extension of K of order p^n, so that $L = K[z]$ and the minimal polynomial of z over K is $x^{p^n} - a$ for some a in K.

The regular subgroup $\alpha(G) = M$ of Perm(G) yields a K-Hopf algebra action on L by the K-Hopf algebra $H = LM^G$, whose structure is determined by how G acts on L and on how $\lambda(G)$ acts on M. The action of G on L is given. In our case $L = K[z]$ is a Kummer extension of K, so the action is transparent. The action of $\lambda(G)$ on M is also straightforward.

Proposition 6. *Let $G = \mathbb{Z}/p^n\mathbb{Z}$, p odd. Suppose $\beta : G \to \mathrm{Hol}(G)$ is a regular embedding with $\beta(1) = (-1, g)$ where $g = 1 + dp$ as in Proposition 2. Then the group $\alpha(G) = M = \langle\eta\rangle$ where $\eta = \alpha(1) = C(b^{-1})(\lambda(1))$. The group M is normalized by $\lambda(G)$ in* Perm(G). *In fact, the action of $\lambda(G)$ on M is induced by $\lambda(1)\eta\lambda(1)^{-1} = \eta^g$.*

Proof. We know that $\eta = C(b^{-1})(\lambda(1))$, and we showed in Lemma 3 that

$$(-1,g)\lambda(1)(-1,g)^{-1} = \lambda(g\cdot 1).$$

When we translate to Perm(G) via $C(b^{-1})$, we obtain

$$C(b^{-1})(-1,g)C(b^{-1})(\lambda(1))C(b^{-1})(-1,g)^{-1} = C(b^{-1})(\lambda(1))^g,$$

that is,

$$C(b^{-1})(-1,g)\eta C(b^{-1})(-1,g)^{-1} = \eta^g,$$

using multiplicative notation for composition of permutations in Perm(G). Now for t in $G = \mathbb{Z}/p^n\mathbb{Z}$, we have

$$b(t) = \frac{g^t - 1}{g - 1},$$

and

$$\begin{aligned} C(b^{-1})(-1,g)(t) &= b^{-1}(-1,g)b(t) \\ &= b^{-1}(-1,g)\left(\frac{g^t-1}{g-1}\right) \\ &= b^{-1}\left(g\left(\frac{g^t-1}{g-1}\right)+1\right) \\ &= b^{-1}\left(\frac{g^{t+1}-1}{g-1}\right) \\ &= b^{-1}(b(t+1)) \\ &= t+1. \end{aligned}$$

So $C(b^{-1})(-1,g) = \lambda(1)$. Thus

$$\lambda(1)\eta\lambda(1)^{-1} = \eta^g. \qquad \square$$

Translating to multiplicative notation for the Galois group $G = \langle\sigma\rangle \cong \mathbb{Z}/p^n\mathbb{Z}$ of the Kummer extension $L|K$, let $\alpha(G) = M = \langle\eta\rangle$ as in Proposition 6. The action of G on LM is induced by the Galois action of G on L and the action on M by $\sigma(\eta) = \lambda(\sigma)\eta\lambda(\sigma)^{-1} = \eta^g$. Thus Proposition 6 enables us to determine the K-Hopf algebra $H = LM^G$ acting on L.

As a K-module we can determine a set of generators of H by simply taking the sums of elements in the distinct orbits under the action of G of $z^k\eta^l$ for all k,l with $0 \le k,l \le p^n-1$. But we are interested in H as a K-algebra, so our objective in the remainder of the paper is to obtain an economical set of generators of H as a K-algebra.

As an initial model, we first do the known case where $G = \langle\sigma\rangle$ is cyclic of order p^2.

6.1. G of order p^2. We suppose L is a cyclic Kummer extension of K of order p^2 with Galois group $G = \langle\sigma\rangle$. Thus K contains a primitive p^2-root of unity ζ, and $L = K[z]$ with $\sigma(z) = \zeta z$, where the minimal polynomial of z over K is $x^{p^2} - a$. Let $M = \langle\eta\rangle$ be cyclic of order p^2 where $\sigma(\eta) = \eta^g$ with $g = 1 + dp$. Then $\sigma(\eta^p) = \eta^p$, so η^p is in $LM^G = H$. Therefore the minimal idempotents

$$e_s^1 = \frac{1}{p}\sum_{i=0}^{p-1}\zeta^{-spi}\eta^{pi}$$

of $K[\langle\eta^p\rangle]$ for $s = 0,\dots,p-1$ are fixed by G. These idempotents satisfy $\eta^p e_s^1 = \zeta^{sp}e_s^1$. It follows that

$$\begin{aligned} \sigma(z^{-sdp}e_s^1\eta) &= \zeta^{-sdp}z^{-sdp}e_s^1\eta^{1+dp} \\ &= \zeta^{-sdp}z^{-sdp}e_s^1\eta^{dp}\eta \\ &= z^{-sdp}e_s^1\eta. \end{aligned}$$

So following the construction of Greither [Gr92], we let

$$a_v = \sum_{s=0}^{p-1} v^s e_s^1$$

where $v = z^{-dp}$. Then

$$\sigma(a_v\eta) = a_v\eta.$$

Proposition 7. *$H = LM^G = K[\eta^p, a_v\eta]$ where $v = z^{-dp}$.*

Proof. Since H has dimension p^2 over K and $K[\eta^p] = \sum_{s=0}^{p-1} Ke_s^1$ is a subalgebra of H, it suffices to show that for $s = 0, \dots, p-1$, $K[\eta^p, a_v\eta]e_s^1$ has dimension p over Ke_s^1. Now

$$K[\eta^p, a_v\eta]e_s^1 = K[a_v\eta]e_s^1 = K[z^{-sdp}\eta]e_s^1,$$

the elements $\{(z^{-sdp}e_s^1\eta)^r : 0 \le r < p\}$ are linearly independent over Ke_s^1, and

$$(z^{-sdp}e_s^1\eta)^p = z^{-p^2sd}\zeta^{sp}e_s^1$$

is in Ke_s^1. Thus for each s, $K[\eta^p, a_v\eta]e_s^1$ has dimension p over Ke_p^1. Hence $K[\eta^p, a_v\eta]$ has dimension p^2 over K and is a subalgebra of H, hence is equal to H. □

This result is in [Ch96, Section 1].

6.2. *G* of order *p^3*. To preview the main result, Theorem 12 below, we write down the result for $L|K$ a Kummer extension with Galois group G, cyclic of order p^3.

In KG we have the idempotents

$$e_t^1 = \frac{1}{p^2}\sum_{j=0}^{p^2-1} \zeta^{-pjt}\eta^{pj}$$

for $0 \le t < p^2$, and

$$e_t^2 = \frac{1}{p}\sum_{j=0}^{p-1} \zeta^{-p^2jt}\eta^{p^2j}$$

for $0 \le t < p$. Then e_t^2 is G-invariant for all t, and e_t^1 is G-invariant if p divides t.

For $\sigma(\eta) = \eta^{1+dp}$ with $(p, d) = 1$, then, analogous to the Greither element for the p^2-case, we let

$$g_{1,sp} = z^{-sdp^2}e_{sp}^1\eta, \text{ for } 0 \le s \le p-1, \text{ and}$$

$$g_{1,s} = \sum_{i=0}^{p-1} \sigma^i(z^{-sdp}e_s^1\eta) \text{ for } 1 \le s \le p-1,$$

the sum of the conjugates of $z^{-sdp}e_s^1\eta$, and let

$$h = \sum_{s=1}^{p-1} g_{1,s} + \sum_{s=0}^{p-1} g_{1,sp}.$$

Then Theorem 12 shows that

$$LM^G = K[h, \eta^{p^2}, e_0^2\eta^p, e_0^1\eta].$$

For $\sigma(\eta) = \eta^{1+dp^2}$, Theorem 12 specializes to show that

$$LM^G = K[h, \eta^p, e_0^2\eta]$$

where

$$h = \sum_{s=0}^{p^2-1} g_{1,s} = \sum_{s=0}^{p^2-1} z^{-sdp^2} e_s^1\eta.$$

6.3. G of order p^n. Let $L = K[z]$, a cyclic Kummer extension of fields of order p^n with Galois group $G = \langle\sigma\rangle$ as at the beginning of Section 6. Let $M = \langle\eta\rangle$ be the regular subgroup of $\mathrm{Perm}(G)$ normalized by G corresponding to the regular embedding $\beta : G \to \mathrm{Hol}(G)$ where $\beta(G) = \langle(-1, 1 + dp^\nu)\rangle$ with $(d, p) = 1$ and $\nu \geq 1$. Then the corresponding K-Hopf algebra acting on L is LM^G, where G acts on L via the Galois action and acts on M by $\sigma(\eta) = \eta^{1+dp^\nu}$.

Idempotents. To obtain a set of algebra generators for LM^G, we first look at the idempotents of KM.

For $r = 0, \ldots, n-1$ and t modulo p^{n-r} we have the pairwise orthogonal idempotents of $K[\eta^{p^r}]$,

$$e_t^r = \frac{1}{p^{n-r}} \sum_{i=0}^{p^{n-r}-1} \zeta^{-tp^r i} \eta^{p^r i}.$$

Then

$$\eta^{p^r} e_t^r = \zeta^{p^r t} e_t^r$$

so for all $k \geq r$,

$$\eta^{sp^k} e_t^r = \zeta^{stp^k} e_t^r,$$

and

$$1 = \sum_{t=0}^{p^{n-r}-1} e_t^r.$$

More generally, the idempotents of $K[\eta^{p^{r+1}}]$ decompose in $K[\eta^{p^r}]$ as:

Lemma 8. *For $r = 0, \ldots, n-2$,*

$$\sum_{k=0}^{p-1} e_{t+kp^{n-r-1}}^r = e_t^{r+1}.$$

Proof.

$$\sum_{k=0}^{p-1} e^r_{t+kp^{n-r-1}} = \frac{1}{p^{n-r}} \sum_{k=0}^{p-1} \sum_{i=0}^{p^{n-r}-1} \zeta^{-p^r i(t+kp^{n-r-1})} \eta^{p^r i}$$
$$= \frac{1}{p^{n-r}} \sum_{i=0}^{p^{n-r}-1} \eta^{p^r i} \zeta^{-p^r it} \sum_{k=0}^{p-1} \zeta^{-ikp^{n-1}}.$$

and the last sum $= 0$ if $i \not\equiv 0$ modulo p, and $= p$ if $i = pj$. So

$$\sum_{k=0}^{p-1} e^r_{t+kp^{n-r-1}} = \frac{1}{p^{n-r-1}} \sum_{j=0}^{p^{n-r-1}-1} \zeta^{-p^{r+1}jt} \eta^{p^{r+1}j} = e^{r+1}_t. \qquad \square$$

Corollary 9. *For all $k > 0$ and all s, t, r,*

$$e^r_s e^{r+k}_t = 0 \text{ if } t \not\equiv s \pmod{p^{n-r-k}}$$
$$= e^r_s \text{ if } t \equiv s \pmod{p^{n-r-k}}.$$

Proof. Since $e^{r+1}_s = e^{r+1}_s e^{r+1}_s$, Lemma 8 gives

$$\sum_{k=0}^{p-1} e^r_{s+kp^{n-r-1}} = \sum_{k=0}^{p-1} e^{r+1}_s e^r_{s+kp^{n-r-1}}.$$

Multiplying both sides by e^r_s, we get

$$e^r_s = e^{r+1}_s e^r_s$$

by pairwise orthogonality of the idempotents $\{e^r_s : s = 0, \ldots, p^{n-r} - 1\}$. Since the subscript t of e^{r+1}_t is defined modulo p^{n-r-1}, the result is then clear for $k = 1$. For general $k > 0$, we can use the case $k = 1$ to write

$$e^r_s = e^r_s e^{r+1}_s \cdots e^{r+k}_s.$$

Then $e^{r+k}_t e^r_s = e^r_s$ iff

$$e^{r+k}_s = e^{r+k}_t,$$

iff

$$s \equiv t \pmod{p^{n-r-k}},$$

and equals 0 otherwise. $\square$

The group $G = \langle \sigma \rangle$ acts on the idempotents by

$$\sigma(e^r_t) = e^r_{t(1+dp^\nu)^{-1}},$$

where the subscript $t(1+dp^\nu)^{-1}$ is modulo p^{n-r}. To verify this G-action, the change of variables $j = i(1+dp^\nu)$ gives

$$\begin{aligned}\sigma(e_t^r) &= \frac{1}{p^{n-r}} \sum_{i=0}^{p^{n-r}-1} \zeta^{-tp^r i} \eta^{p^r i(1+dp^\nu)} \\ &= \frac{1}{p^{n-r}} \sum_{j=0}^{p^{n-r}-1} \zeta^{-tp^r j(1+dp^\nu)^{-1}} \eta^{p^r j} \\ &= e^r_{t(1+dp^\nu)^{-1}}.\end{aligned}$$

For $t = sp^\epsilon$ with s coprime to p and for $k \geq 0$, we have

$$\sigma^{p^k}(e^r_{sp^\epsilon}) = e^r_{sp^\epsilon(1+dp^\nu)^{-p^k}}.$$

The subscript t on e_t^r is modulo p^{n-r}, and for $k = n-r-\epsilon-\nu$,

$$sp^\epsilon(1+dp^\nu)^{-p^k} \equiv sp^\epsilon \pmod{p^{n-r}}.$$

Hence

$$\sigma^{p^{(n-r-\epsilon-\nu)}}(e^r_{sp^\epsilon}) = e^r_{sp^\epsilon}.$$

In particular, for $r = n-\epsilon-\nu$ and $\epsilon = 0, \ldots, n-1-\nu$, we have

$$\sigma(e^{n-\nu-\epsilon}_{sp^\epsilon}) = e^{n-\nu-\epsilon}_{sp^\epsilon}.$$

We may now write 1 as a sum of pairwise orthogonal G-invariant idempotents:

Proposition 10. *In LM^G, we have*

$$1 = \sum_{\epsilon=0}^{n-\nu-2} \sum_{s=1,(s,p)=1}^{p^\nu-1} e^{n-\nu-\epsilon}_{sp^\epsilon} + \sum_{s=1}^{p^\nu-1} e^1_{sp^{n-\nu-1}}.$$

Proof. We just observed that all of the idempotents in the sum are fixed by G.

We have

$$1 = \sum_{s=0}^{p^\nu-1} e_s^{n-\nu} = \sum_{s=1,(s,p)=1}^{p^\nu-1} e_s^{n-\nu} + \sum_{r=0}^{p^{\nu-1}-1} e_{rp}^{n-\nu}.$$

Now by Lemma 8,

$$e_{rp}^{n-\nu} = \sum_{k=0}^{p-1} e^{n-\nu-1}_{rp+kp^\nu},$$

also a sum of pairwise orthogonal idempotents, so

$$\begin{aligned}\sum_{r=0}^{p^{\nu-1}-1} e_{rp}^{n-\nu} &= \sum_{r=0}^{p^{\nu-1}-1}\sum_{k=0}^{p-1} e_{rp+kp^\nu}^{n-\nu-1}\\ &= \sum_{t=0}^{p^\nu-1} e_{tp}^{n-\nu-1}\\ &= \sum_{s=1,(s,p)=1}^{p^\nu-1} e_{sp}^{n-\nu-1} + \sum_{r=0}^{p^{\nu-1}-1} e_{rp^2}^{n-\nu-1}.\end{aligned}$$

Repeating this decomposition $n-\nu-2$ more times yields the desired formula. □

Generators. We want to find generators of $LM^G e_{sp^\epsilon}^{n-\nu-\epsilon}$ over $Ke_{sp^\epsilon}^{n-\nu-\epsilon}$. By analogy with the p^2 case, which involves the sum of Greither generators $z^{-sdp}e_s^1\eta$, we look at elements of the form

$$z^k e_{sp^\epsilon}^r \eta^{p^{r-1}}$$

with $(s,p)=1$. For $n=2$, the summands $z^{-sdp}e_s^1\eta$ are fixed by G. For $n>2$ what are fixed are sums of conjugates under the action of G. We therefore need to know what power of σ fixes these elements.

Proposition 11. *We have*

$$\sigma^{p^{n-r-\epsilon-\nu}}(z^{-sdp^{\epsilon+r+\nu-1}}e_{sp^\epsilon}^r\eta^{p^{r-1}}) = z^{-sdp^{\epsilon+r+\nu-1}}e_{sp^\epsilon}^r\eta^{p^{r-1}}.$$

Proof. We have

$$\sigma^{p^{n-r-\epsilon-\nu}}(z^{-sdp^{\epsilon+r+\nu-1}}) = \zeta^{-sdp^{n-1}}z^{-sdp^{\epsilon+r+\nu-1}}$$

while

$$\sigma^{p^{n-r-\epsilon-\nu}}(e_{sp^\epsilon}^r) = e_{sp^\epsilon}^r$$

and $\sigma(\eta)=\eta^{1+dp}$. So

$$\sigma^{p^{n-r-\epsilon-\nu}}(e_{sp^\epsilon}^r\eta^{p^{r-1}}) = e_{sp^\epsilon}^r\eta^{p^{r-1}(1+dp^\nu)^k}$$

where $k=p^{n-r-\epsilon-\nu}$. The exponent of η is

$$\begin{aligned}p^{r-1}(1+dp^\nu)^{p^{n-r-\epsilon-\nu}} &= p^{r-1}+p^{n-r-\epsilon-\nu}p^{r-1}dp^\nu + d'p^{n-r-\epsilon-\nu}p^{r-1}p^{2\nu}\\ &= p^{r-1}+dp^{n-\epsilon-1}+d''p^{n-\epsilon}\end{aligned}$$

for some d''. So since $r\le n-\epsilon-\nu\le n-\epsilon-1$,

$$\begin{aligned}\sigma^{p^{n-r-\epsilon-\nu}}(e_{sp^\epsilon}^r\eta^{p^{r-1}}) &= e_{sp^\epsilon}^r\eta^{p^{r-1}+dp^{n-\epsilon-1}+d''p^{n-\epsilon}}\\ &= \zeta^{sdp^{n-1}}e_{sp^\epsilon}^r\eta^{p^{r-1}}.\end{aligned}$$

The respective powers of ζ cancel to give the result. □

Now we can define the generators of the K-Hopf algebra LM^G.

For $0 \le \epsilon \le n-\nu-1$, $1 \le r \le n-\epsilon-\nu$, and $1 \le s \le p-1$, let g_{r,sp^ϵ} be the sum of the conjugates of the Greither elements $z^{-sdp^{\epsilon+r+\nu-1}} e^r_{sp^\epsilon} \eta^{p^{r-1}}$:

$$g_{r,sp^\epsilon} = \sum_{i=0}^{p^{n-\epsilon-r-\nu}-1} \sigma^i(z^{-sdp^{\epsilon+r+\nu-1}} e^r_{sp^\epsilon} \eta^{p^{r-1}}).$$

Then g_{r,sp^ϵ} is fixed by G for all s by Proposition 11, so lies in LM^G. In particular,

$$g_{1,sp^\epsilon} = \sum_{i=0}^{p^{n-\epsilon-\nu-1}-1} \sigma^i(z^{-sdp^{\epsilon+\nu}} e^1_{sp^\epsilon} \eta),$$

while

$$g_{n-\epsilon-\nu,sp^\epsilon} = z^{-sdp^{n-1}} e^{n-\epsilon-\nu}_{sp^\epsilon} \eta^{p^{n-\epsilon-\nu-1}}.$$

We set h to be the sum of all the sums of conjugates with $r = 1$:

$$h = \sum_{\epsilon=0}^{n-\nu-2} \sum_{s=1,(s,p)=1}^{p^\nu-1} g_{1,sp^\epsilon} + \sum_{s=0}^{p^\nu-1} g_{1,sp^{n-\nu-1}}.$$

Recall that $\sigma(\eta) = \eta^{1+dp^\nu}$ with $(d,p) = 1$ and $\nu \ge 1$. Thus $\eta^{p^{n-\nu}}$ is in LM^G since $\sigma(\eta^{p^{n-\nu}}) = \eta^{p^{n-\nu}(1+dp^\nu)} = \eta^{p^{n-\nu}}$. Also, for $r = \nu, \dots, n-1$, $e^r_0 \eta^{p^{r-\nu}}$ is in LM^G, for $\sigma(e^r_0) = e^r_0$ and so

$$\sigma(e^r_0 \eta^{p^{r-\nu}}) = e^r_0 \eta^{p^{r-\nu}(1+dp^\nu)} = e^r_0 \eta^{p^{r-\nu}} \eta^{p^r d} = e^r_0 \eta^{p^{r-\nu}}$$

since $e^r_0 \eta^{p^r} = e^r_0$.

Let

$$H = K[h, \eta^{p^{n-\nu}}, e^{n-1}_0 \eta^{p^{n-1-\nu}}, \dots, e^r_0 \eta^{p^{r-\nu}}, \dots, e^\nu_0 \eta].$$

Evidently, $H \subset LM^G$.

The main result. We show that the algebra generators of H generate all of LM^G:

Theorem 12. *$H = LM^G$.*

Proof. The idea of the proof is to take the idempotents in Proposition 10, break up $K[h]$ into a direct product corresponding to those idempotents, and count the dimensions over K of the direct factors.

We first show that the idempotents $e^{n-\nu-\epsilon}_{sp^\epsilon}$ appearing in Proposition 10 are in H. For $\epsilon = 1, \dots, n-\nu-1$, we have

$$e^{n-\nu-\epsilon}_{sp^\epsilon} = e^{n-\epsilon}_0 e^{n-\nu-\epsilon}_{sp^\epsilon}$$

by Corollary 9. Since

$$e^{n-\nu-\epsilon}_{sp^\epsilon} = \frac{1}{p^{\nu+\epsilon}} \sum_{j=0}^{p^{\nu+\epsilon}-1} \zeta^{-jsp^{n-\nu}} \eta^{jp^{n-\nu-\epsilon}},$$

we may multiply both sides by $e_0^{n-\epsilon}$ to get

$$e_{sp^\epsilon}^{n-\nu-\epsilon} = \frac{1}{p^{\nu+\epsilon}} \sum_{j=0}^{p^{\nu+\epsilon}-1} \zeta^{-jsp^{n-\nu}} e_0^{n-\epsilon} (\eta^{p^{n-\nu-\epsilon}})^j,$$

a K-linear combination of powers of $e_0^{n-\epsilon}\eta^{p^{n-\nu-\epsilon}}$, hence in H. For $\epsilon = 0$, the idempotents $e_s^{n-\nu}$ are K-linear combinations of powers of $\eta^{p^{n-\nu}}$, hence are in H.

Now by Proposition 10, 1 decomposes into a sum of pairwise orthogonal G-invariant idempotents:

$$1 = \sum_{\epsilon=0}^{n-\nu-2} \sum_{s=1,(s,p)=1}^{p^\nu-1} e_{sp^\epsilon}^{n-\nu-\epsilon} + \sum_{s=0}^{p^\nu-1} e_{sp^{n-\nu-1}}^{1}.$$

We also have

$$h = \sum_{\epsilon=0}^{n-\nu-2} \sum_{s=1,(s,p)=1}^{p^\nu-1} g_{1,sp^\epsilon} + \sum_{s=0}^{p^\nu-1} g_{1,sp^{n-\nu-1}}.$$

We show:

Proposition 13. *For all pairs (s,ϵ) with s coprime to p and $0 \le \epsilon \le n-\nu-2$ or with $\epsilon = n-\nu-1$, we have*

$$h e_{sp^\epsilon}^{n-\nu-\epsilon} = g_{1,sp^\epsilon}.$$

Proof. For each pair (t,f) we have

$$h e_{tp^f}^{n-\nu-f} = \sum_{\epsilon=0}^{n-\nu-2} \sum_{s=1,(s,p)=1}^{p^\nu-1} g_{1,sp^\epsilon} e_{tp^f}^{n-\nu-f} + \sum_{s=0}^{p^\nu-1} g_{1,sp^{n-\nu-1}} e_{tp^f}^{n-\nu-f}.$$

We have four cases to show.

Case 1. If $n-\nu-f \ge 2$ and t is coprime to p, then

$$g_{1,sp^{n-\nu-1}} e_{tp^f}^{n-\nu-f} = 0.$$

Case 2.

$$g_{1,sp^{n-\nu-1}} e_{tp^{n-\nu-1}}^{1} = 0$$

if $t \ne s$, while

$$g_{1,sp^{n-\nu-1}} e_{sp^{n-\nu-1}}^{1} = g_{1,sp^{n-\nu-1}}.$$

Case 3. For s coprime to p and $n-\nu-\epsilon \ge 2$,

$$g_{1,sp^\epsilon} e_{tp^{n-\nu-1}}^{1} = 0$$

for all t.

Case 4. For s, t coprime to p and $\epsilon, f \le n-\nu-2$,

$$g_{1,sp^\epsilon} e_{tp^f}^{n-\nu-f} = 0$$

if $f \ne \epsilon$ or if $f = \epsilon$ but $t \ne s$, while

$$g_{1,sp^\epsilon} e_{sp^\epsilon f}^{n-\nu-\epsilon} = g_{1,sp^\epsilon}.$$

We use Corollary 9: For all $k > 0$ and all s, t, r,

$$\begin{aligned} e_s^r e_t^{r+k} &= 0 \text{ if } t \not\equiv s \pmod{p^{n-r-k}} \\ &= e_s^r \text{ if } t \equiv s \pmod{p^{n-r-k}}. \end{aligned}$$

Case 1: We have $n-\nu-f \ge 2$ and t is coprime to p. Now

$$g_{1,sp^{n-\nu-1}} e_{tp^f}^{n-\nu-f} = z^{-sdp^{n-1}} \eta e^1_{sp^{n-\nu-1}} e_{tp^f}^{n-\nu-f},$$

and by Proposition 8, this $\ne 0$ if $sp^{n-\nu-1} \equiv tp^f \pmod{p^{n-(n-\nu-f)}}$. But since

$$\operatorname{ord}_p(tp^f) = f \le n-\nu-2 < \operatorname{ord}_p(sp^{n-\nu-1})$$

the congruence never holds, so Case 1 is true.

Case 2: Since $g_{1,sp^{n-\nu-1}}$ is a multiple of $e^1_{sp^{n-\nu-1}}$, Case 2 follows from the orthogonality of the idempotents $\{e^1_{tp^{n-\nu-1}}\}$.

For Cases 3 and 4 we assume s is coprime to p and $n-\nu-\epsilon \ge 2$. We write

$$\begin{aligned} g_{1,sp^\epsilon} &= \sum_{i=0}^{p^{n-\epsilon-\nu-1}-1} \sigma^i(z^{-sdp^{\epsilon+\nu}} \eta e^1_{sp^\epsilon}) \\ &= \sum_{i=0}^{p^{n-\epsilon-\nu-1}-1} z^{-sdp^{\epsilon+\nu}} \zeta^{-sdp^{\epsilon+\nu}} \eta^{(1+dp^\nu)^i} e^1_{sp^\epsilon(1+dp^\nu)^{-i}} \\ &= \sum_{i=0}^{p^{n-\epsilon-\nu-1}-1} \gamma_i e^1_{sp^\epsilon(1+dp^\nu)^{-i}} \end{aligned}$$

where γ_i is the coefficient of $e^1_{sp^\epsilon(1+dp^\nu)^{-i}}$ in the ith summand.

Case 3 is the case

$$g_{1,sp^\epsilon} e^1_{tp^{n-\nu-1}} = \sum_{i=0}^{p^{n-\epsilon-\nu-1}-1} \gamma_i e^1_{sp^\epsilon(1+dp^\nu)^{-i}} e^1_{tp^{n-\nu-1}},$$

which $= 0$ from Corollary 9 by essentially the same argument as in Case 1.

Case 4: For t coprime to p and $n-\nu-f \ge 2$, we have

$$g_{1,sp^\epsilon} e_{tp^f}^{n-\nu-f} = \sum_{i=0}^{p^{n-\epsilon-\nu-1}-1} \gamma_i e^1_{sp^\epsilon(1+dp^\nu)^{-i}} e_{tp^f}^{n-\nu-f}.$$

The term

$$\gamma_i e^1_{sp^\epsilon(1+dp^\nu)^{-i}} e_{tp^f}^{n-\nu-f} = 0 \text{ or } = \gamma_i e^1_{sp^\epsilon(1+dp^\nu)^{-i}}$$

depending on whether or not

$$sp^\epsilon(1+dp^\nu)^{-i} \equiv tp^f \pmod{p^{n-(n-\nu-f)}}$$

that is,

$$sp^\epsilon \equiv tp^f(1+dp^\nu)^i \pmod{p^{\nu+f}}.$$

Since s and t are coprime to p, this congruence can hold exactly when $\epsilon = f$ and $s \equiv t \pmod{p^\nu}$, independent of i. Thus $g_{1,sp^\epsilon} e_{tp^f}^{n-\nu-f} = g_{1,sp^\epsilon}$ precisely when $f = \epsilon$ and $t \equiv s \pmod{p^\nu}$, and $= 0$ otherwise. The proposition follows. □

By Proposition 13,

$$He_{sp^\epsilon}^{n-\nu-\epsilon} \supseteq K[h]e_{sp^\epsilon}^{n-\nu-\epsilon} = K[g_{1,sp^\epsilon}]e_{sp^\epsilon}^{n-\nu-\epsilon}.$$

Now H decomposes into a direct sum of subrings corresponding to the idempotents arising in Proposition 10:

$$H = \sum_{\epsilon=0}^{n-\nu-2} \sum_{s=1,(s,p)=1}^{p^\nu-1} He_{sp^\epsilon}^{n-\nu-\epsilon} + \sum_{s=1}^{p^\nu-1} He_{sp^{n-\nu-1}}^{1},$$

so

$$H \supseteq \sum_{\epsilon=0}^{n-\nu-2} \sum_{s=1,(s,p)=1}^{p^\nu-1} K[g_{1,sp^\epsilon}]e_{sp^\epsilon}^{n-\nu-\epsilon} + \sum_{s=1}^{p^\nu-1} K[g_{1,sp^{n-\nu-1}}]e_{sp^{n-\nu-1}}^{1},$$

a module over

$$\sum_{\epsilon=0}^{n-\nu-2} \sum_{s=1,(s,p)=1}^{p^\nu-1} Ke_{sp^\epsilon}^{n-\nu-\epsilon} + \sum_{s=1}^{p^\nu-1} Ke_{sp^{n-\nu-1}}^{1}.$$

We will compute the dimension of $K[g_{1,sp^\epsilon}]e_{sp^\epsilon}^{n-\nu-\epsilon}$ over $Ke_{sp^\epsilon}^{n-\nu-\epsilon}$ for each s, ϵ. The sum of those dimensions is less than or equal to the dimension of H as a K-module. When we show that the sum of the dimensions is p^n, then, since LM^G is known by descent to have dimension p^n and $H \subseteq LM^G$, we will obtain equality.

To compute the desired dimensions, we have

Proposition 14. *For $r = 1, \ldots, n-\epsilon-\nu-1$ and $(s,p) = 1$,*

$$g_{r,sp^\epsilon}^p = g_{r+1,sp^\epsilon}.$$

Proof. Since g_{r,sp^ϵ} is a sum of terms involving pairwise orthogonal idempotents, we have

$$g_{r,sp^\epsilon}^p = \sum_{i=0}^{p^{n-\epsilon-r-\nu}-1} \sigma^i(z^{-sdp^{\epsilon+r+\nu}} e_{sp^\epsilon}^r \eta^{p^r})$$

and

$$e_{sp^\epsilon}^r \eta^{p^r} = \zeta^{sp^{r+\epsilon}} e_{sp^\epsilon}^r.$$

In the summation formula for g^p_{r,sp^ϵ} we write the index of summation in base $p^{n-\epsilon-r-\nu-1}$: $i = j + kp^{n-\epsilon-r-\nu-1}$. Then

$$g^p_{r,sp^\epsilon} = \sum_{j=0}^{p^{n-\epsilon-r-\nu-1}-1} \sigma^j \sum_{k=0}^{p-1} \sigma^{kp^{n-\epsilon-r-\nu-1}}(z^{-sdp^{\epsilon+r+\nu}} e^r_{sp^\epsilon} \zeta^{sp^{r+\epsilon}}).$$

Focusing on the part of the expression for g^p_{r,sp^ϵ} involving the index k, we have

$$\sigma^{kp^{n-\epsilon-r-\nu-1}}(z^{-sdp^{\epsilon+r+\nu}}) = \zeta^{-sdkp^{n-1}} z^{-sdp^{\epsilon+r+\nu}},$$

and

$$\sigma^{kp^{n-\epsilon-r-\nu-1}}(e^r_{sp^\epsilon}) = e^r_{sp^\epsilon - sdkp^{n-r-1}}.$$

To verify this last formula, we see that the subscript of e^r on the left side is

$$sp^\epsilon(1+dp^\nu)^{-kp^{n-\epsilon-r-\nu-1}},$$

and since the subscript t of e^r_t is defined modulo p^{n-r}, that subscript is

$$\begin{aligned} sp^\epsilon(1+dp^\nu)^{-kp^{n-\epsilon-r-\nu-1}} &\equiv sp^\epsilon - sp^\epsilon kp^{n-\epsilon-r-\nu-1}dp^\nu \\ &\equiv sp^\epsilon - skdp^{n-r-1} \pmod{p^{n-r}}. \end{aligned}$$

Thus

$$\begin{aligned} &\sigma^{kp^{n-\epsilon-r-\nu-1}}(z^{-sdp^{\epsilon+r+\nu}} e^r_{sp^\epsilon} \zeta^{sp^{r+\epsilon}}) \\ &\qquad = z^{-sdp^{\epsilon+r+\nu}} e^r_{sp^\epsilon - skdp^{n-r-1}} \zeta^{sp^{r+\epsilon} - skdp^{n-1}}. \end{aligned}$$

Now we observe that

$$\eta^{p^r} e^r_{sp^\epsilon - skdp^{n-r-1}} = \zeta^{sp^{r+\epsilon} - skdp^{n-1}} e^r_{sp^\epsilon - skdp^{n-r-1}}.$$

So

$$\begin{aligned} &z^{-sdp^{\epsilon+r+\nu}} e^r_{sp^\epsilon - skdp^{n-r-1}} \zeta^{sp^{r+\epsilon} - skdp^{n-1}} \\ &\qquad = z^{-sdp^{\epsilon+r+\nu}} \eta^{p^r} e^r_{sp^\epsilon - skdp^{n-r-1}}, \end{aligned}$$

and the sum involving k becomes

$$\begin{aligned} \sum_{k=0}^{p-1} z^{-sdp^{\epsilon+r+\nu}} \eta^{p^r} e^r_{sp^\epsilon - skdp^{n-r-1}} &= z^{-sdp^{\epsilon+r+\nu}} \eta^{p^r} \sum_{k=0}^{p-1} e^r_{sp^\epsilon - skdp^{n-r-1}} \\ &= z^{-sdp^{\epsilon+r+\nu}} \eta^{p^r} e^{r+1}_{sp^\epsilon} \end{aligned}$$

by Lemma 8, since sd is coprime to p. Thus

$$\begin{aligned} g^p_{r,sp^\epsilon} &= \sum_{j=0}^{p^{n-\epsilon-r-\nu-1}-1} \sigma^j (z^{-sdp^{\epsilon+r+\nu}} \eta^{p^r} e^{r+1}_{sp^\epsilon}) \\ &= g_{r+1,sp^\epsilon}. \end{aligned}$$

□

Now we compute the dimension

$$[K[g_{1,sp^\epsilon}] : Ke^{n-\nu-\epsilon}_{sp^\epsilon}]$$

for $(s,p)=1$ and $\epsilon < n-\nu-1$ and for $\epsilon = n-\nu-1$ and all s.

First assume s is coprime to p. We have from Proposition 14 that

$$g^{p^r}_{1,sp^\epsilon} = g_{r+1,sp^\epsilon}$$

for all $r = 1,\dots,n-\epsilon-\nu-1$ and $(s,p)=1$, and so

$$g^{p^{n-\epsilon-\nu-1}}_{1,sp^\epsilon} = g_{n-\epsilon-\nu,sp^\epsilon} = z^{sdp^{n-1}} e^{n-\epsilon-\nu}_{sp^\epsilon} \eta^{p^{n-\epsilon-\nu-1}}.$$

Then

$$g^{p^{n-\epsilon-\nu}}_{1,sp^\epsilon} = (g^{p^{n-\epsilon-\nu-1}}_{1,sp^\epsilon})^p = z^{-sdp^n} e^{n-\epsilon-\nu}_{sp^\epsilon} \eta^{p^{n-\epsilon-\nu}}$$

is in $Ke^{n-\epsilon-\nu}_{sp^\epsilon}$. Thus the dimension of $K[g_{1,sp^\epsilon}]$ over $Ke^{n-\epsilon-\nu}_{sp^\epsilon}$ is $\le p^{n-\nu-\epsilon}$.

Now g_{1,sp^ϵ} has the form

$$g_{1,sp^\epsilon} = z^{-sdp^{\epsilon+\nu}} \eta \sum_{i=0}^{p^{n-\epsilon-\nu-r}-1} \zeta^{d_i} e^1_{sp^\epsilon(1+dp^\nu)^{-i}}$$

for some exponent d_i. This is of the form $\theta z^{-sdp^{\epsilon+\nu}}$ where θ is in the group ring $L[\eta]$. Since $L[\eta]$ is a free module over $K[\eta]$ with basis $\{z^j : j = 0,\dots,p^n-1\}$ and $g^{p^{n-\epsilon-\nu}}_{1,sp^\epsilon} \neq 0$ in $K[\eta]$, the set

$$\{g^j_{1,sp^\epsilon} : j = 0\dots, p^{n-\epsilon-\nu}-1\}$$

is linearly independent over $K[\eta]$, hence over $Ke^1_{sp^\epsilon}$.

It follows that for $\epsilon < n-\nu-1$ and s coprime to p, the dimension of $K[g_{1,sp^\epsilon}$ over $Ke^1_{sp^\epsilon}$ is $= p^{n-\nu-\epsilon}$.

For $\epsilon = n-\nu-1$ and all s, we have

$$K[g_{1,sp^{n-\nu-1}}] = K[z^{-sdp^{n-1}} e^1_{sp^{n-\nu-1}}\eta]$$

which clearly has dimension p as a module over $Ke^1_{sp^{n-\nu-1}}$.

Summing these dimensions, the dimension of H over K is

$$\begin{aligned} &\ge \sum_{\epsilon=0}^{n-\nu-2} \sum_{s=1,(s,p)=1}^{p^\nu-1} p^{n-\epsilon-\nu} + \sum_{s=0}^{p^\nu-1} p \\ &= (p^\nu - p^{\nu-1})(p^{n-\nu} + p^{n-\nu-1} + \dots + p^2) + p(p^\nu) = p^n. \end{aligned}$$

Since $H \subseteq LM^G$, we must have $H = LM^G$, completing the proof of Theorem 12. □

Example 15. Let G be cyclic of order 27. Let M be the regular subgroup of $\mathrm{Perm}(G)$ corresponding to the cyclic subgroup $\langle(-1,4)\rangle$. Then $\beta(t) = (-1,4)^t$, so

$$b(t) \equiv \left(\frac{4^t-1}{3}\right) \pmod{27}.$$

One may verify that

$$\begin{aligned} b(3m) &= -2(3m) \\ b(1+3m) &= 1+3m \\ b(2+3m) &= 5+12m \end{aligned}$$

and that

$$\begin{aligned} b^{-1}(-3m) &= -12m = 4(-3m) \\ b^{-1}(-(1+3m)) &= 14+6m \\ b^{-1}(-(2+3m)) &= -2-3m. \end{aligned}$$

Now $LM^G = K[h, \eta^9, e_0^2\eta^3, e_0^1\eta]$ where

$$h = g_{1,1} + g_{1,2} + g_{1,0} + g_{1,3} + g_{1,6}.$$

Using Theorem 12 and Proposition 1, the actions of these generators of H are as follows:

$$\eta^9(a) = \sigma^{b^{-1}(-9)}(a) = \sigma^{-36}(a) = \sigma^{18}(a);$$

$$\begin{aligned} e_0^2\eta^3(a) &= \frac{1}{3}\sum_{k=0}^{2}\eta^{9k+3}(a) = \frac{1}{3}\sum_{k=0}^{2}\sigma^{b^{-1}(-(9k+3))}(a) \\ &= \frac{1}{3}\sum_{k=0}^{2}\sigma^{-4(9k+3))}(a) = \frac{1}{3}\sum_{k=0}^{2}\sigma^{15-9k}(a) \\ &= \frac{1}{3}\sigma^6(a+\sigma^9(a)+\sigma^{18}(a)); \end{aligned}$$

and

$$\begin{aligned} e_0^1\eta(a) &= \frac{1}{9}\sum_{k=0}^{8}\eta^{3k+1}(a) = \frac{1}{9}\sum_{k=0}^{8}\sigma^{b^{-1}(-(3k+1))}(a) \\ &= \frac{1}{9}\sum_{k=0}^{8}\sigma^{14+6k}(a) = \frac{1}{9}\sum_{l=0}^{8}\sigma^{2+3l}(a). \end{aligned}$$

As for the components of h, we have

$$\begin{aligned} g_{1,3s}(a) &= z^{-9s}e_{3s}^1\eta(a) \\ &= \frac{1}{9}\sum_{k=0}^{8}z^{-9s}\zeta^{-9sk}\sigma^{b^{-1}(-3k-1)}(a) \\ &= \frac{1}{9}\sum_{k=0}^{8}z^{-9s}\zeta^{-9sk}\sigma^{14+6k}(a) \end{aligned}$$

for $s = 1, 2$ (note that $g_{1,0} = e_0^1\eta$ was done above), and since

$$\begin{aligned} g_{1,s} &= \sum_{i=0}^{2} \sigma^i(z^{-3s}e_s^1\eta) \\ &= z^{-3s}e_s^1\eta + \zeta^{-3s}z^{-3s}e_{7s}^1\eta^4 + \zeta^{-6s}z^{-3s}e_{22s}^1\eta^{16} \\ &= z^{-3s}\eta(e_s^1 + \zeta^{18s}e_{7s}^1 + e_{22s}^1) \\ &= \frac{1}{9}z^{-3s}\sum_{k=0}^{8}(\zeta^{-3sk} + \zeta^{18s-21sk} + \zeta^{-66k})\eta^{3k+1}, \end{aligned}$$

we have

$$g_{1,s}(a) = \frac{z^{-3s}}{9}\sum_{k=0}^{8}(\zeta^{-3sk} + \zeta^{18s-21sk} + \zeta^{-66k})\sigma^{14+6k}(a)$$

for $s = 1, 2$.

References

[By96] Byott, Nigel P. Uniqueness of Hopf Galois structure for separable field extensions. *Comm. Algebra* **24** (1996), 3217–3228. MR1402555 (97j:16051a), Zbl 0878.12001. Corrigendum. *Comm. Algebra* **24** (1996), 3705. MR1405283 (97j:16051b).

[By97a] Byott, Nigel P. Galois structure of ideals in wildly ramified abelian p-extensions of a p-adic field, and some applications. *J. Théor. Nombres Bordeaux* **9** (1997), 201–219. MR1469668 (98h:11152), Zbl 0889.11040.

[By97b] Byott, Nigel P. Associated orders of certain extensions arising from Lubin–Tate formal groups. *J. Théor. Nombres Bordeaux* **9** (1997), no. 2, 449–462. MR1617408 (99d:11126), Zbl 0902.11052.

[By99] Byott, Nigel P. Integral Galois module structure of some Lubin–Tate extensions. *J. Number Theory* **77** (1999), no. 2, 252–273. MR1702149 (2000f:11156), Zbl 0937.11057.

[By00] Byott, Nigel P. Galois module structure and Kummer theory for Lubin–Tate formal groups. *Algebraic number theory and Diophantine analysis* (Graz, 1998), 55–67. *de Gruyter, Berlin*, 2000. MR1770454 (2001h:11148), Zbl 0958.11076.

[By02] Byott, Nigel P. Integral Hopf–Galois structures on degree p^2 extensions of p-adic fields. *J. Algebra* **248** (2002), no. 1, 334–365. MR1879021 (2002j:11142), Zbl 0992.11065.

[By04a] Byott, Nigel P. Hopf–Galois structures on field extensions with simple Galois groups. *Bull. London Math. Soc.* **36** (2004), 23–29. MR2011974 (2004i:16049), Zbl 1038.12002.

[By04b] Byott, Nigel P. Hopf–Galois structures on Galois field extensions of degree pq. *J. Pure Appl. Algebra* **188** (2004), 45–57. MR2030805 (2004j:16041), Zbl 1047.16022.

[By07] Byott, Nigel P. Hopf–Galois structures on almost cyclic field extensions of 2-power degree. *J. Algebra* **318** (2007), 351–371. MR2363137 (2009a:12006), Zbl 1183.12002.

[CaC99] Carnahan, Scott; Childs, Lindsay. Counting Hopf Galois structures on non-abelian Galois field extensions. *J. Algebra* **218** (1999), 81–92. MR1704676 (2000e:12010), Zbl 0988.12003.

[CS69] Chase, Stephen U.; Sweedler, Moss E. Hopf algebras and Galois theory. Lecture Notes in Mathematics, 97. *Springer-Verlag, Berlin-New York*, 1969. ii+133 pp. MR0260724 (41 #5348), Zbl 0197.01403.

[Ch89] Childs, Lindsay N. On the Hopf Galois theory for separable field extensions. *Comm. Algebra* **17** (1989), 809–825. MR0990979 (90g:12003), Zbl 0692.12007.

[Ch96] Childs, Lindsay N. Hopf Galois structures on degree p^2 cyclic extensions of local fields. *New York J. Mathematics* **2** (1996), 86–102. MR1420597 (97j:11058), Zbl 0884.11046.

[Ch00] 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.

[Ch03] Childs, Lindsay N. On Hopf Galois structures and complete groups. *New York J. Mathematics* **9** (2003), 99–116. MR2016184 (2004k:16097), Zbl 1038.12003.

[Ch05] Childs, Lindsay N. Elementary abelian Hopf Galois structures and polynomial formal groups. *J. Algebra* **283** (2005), 292–316. MR2102084 (2005g:16073), Zbl 1071.16031.

[Ch07] Childs, Lindsay N. Some Hopf Galois structures arising from elementary abelian p-groups. *Proc. Amer. Math. Soc.* **135** (2007), 3453–3460. MR2336557 (2008j:16107), Zbl 1128.16022.

[CCo07] Childs, Lindsay N.; Corradino, Jesse. Cayley's theorem and Hopf Galois structures for semidirect products of cyclic groups. *J. Algebra* **308** (2007), 236–251. MR2290920 (2007j:20026), Zbl 1119.16037.

[CM94] Childs, Lindsay N.; Moss, David J. Hopf algebras and local Galois module theory. *Advances in Hopf Algebras* (Chicago, IL, 1992), 1–24. Lecture Notes in Pure and Appl. Math., 158. *Dekker, New York*, 1994. MR1289419 (95g:11116), Zbl 0826.16035.

[Co00] Cohen, Henri. Advanced topics in computational number theory. Graduate Texts in Mathematics, 193. *Springer-Verlag, New York*, 2000. xvi+578 pp. ISBN: 0-387-98727-4. MR1728313 (2000k:11144), Zbl 0977.11056.

[FCC11] Featherstonhaugh, S. C.; Caranti, A.; Childs, L. N. Abelian Hopf Galois structures on prime-power Galois field extensions. *Trans. Amer. Math. Soc.*, to appear.

[Gr92] Greither, Cornelius. Extensions of finite group schemes, and Hopf Galois theory over a complete discrete valuation ring. *Math. Z.* **210** (1992), 37–67. MR1161169 (93f:14024), Zbl 0737.11038.

[GP87] Greither, Cornelius; Pareigis, Bodo. Hopf Galois theory for separable field extensions. *J. Algebra* **106** (1987), 239–258. MR0878476 (88i:12006), Zbl 0615.12026.

[Ko98] Kohl, Timothy. Classification of the Hopf Galois structures on prime power radical extensions. *J. Algebra* **207** (1998), 525–546. MR1644203 (99g:16049), Zbl 0953.12003.

[Ko07] Kohl, Timothy. Groups of order $4p$, twisted wreath products and Hopf–Galois theory. *J. Algebra* **314** (2007), 42–74. MR2331752 (2008e:12001), Zbl 1129.16031.

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

This paper is available via http://nyjm.albany.edu/j/2011/17-4.html.