Isomorphism problems for Hopf-Galois structures on separable field extensions

Alan Koch[a], Timothy Kohl[b], Paul J. Truman[c,*], Robert Underwood[d]

[a]*Department of Mathematics, Agnes Scott College, 141 E. College Ave., Decatur, GA 30030 USA*
[b]*Department of Mathematics and Statistics, Boston University, 111 Cummington Mall, Boston, MA 02215 USA*
[c]*School of Computing and Mathematics, Keele University, Staffordshire, ST5 5BG, UK*
[d]*Department of Mathematics and Computer Science, Auburn University at Montgomery, Montgomery, AL, 36124 USA*

Abstract

Let L/K be a finite separable extension of fields whose Galois closure E/K has Galois group G. Greither and Pareigis use Galois descent to show that a Hopf algebra giving a Hopf-Galois structure on L/K has the form $E[N]^G$ for some group N of order $[L : K]$. We formulate criteria for two such Hopf algebras to be isomorphic as Hopf algebras, and provide a variety of examples. In the case that the Hopf algebras in question are commutative, we also determine criteria for them to be isomorphic as K-algebras. By applying our results, we complete a detailed analysis of the distinct Hopf algebras and K-algebras that appear in the classification of Hopf-Galois structures on a cyclic extension of degree p^n, for p an odd prime number.

Keywords: Hopf-Galois extension, Greither-Pareigis theory, Galois descent
2000 MSC: 16T05

1. Introduction

Let L/K be a finite extension of fields and H a K-Hopf algebra. We say that L is an *H-Galois extension of K*, or that H gives a *Hopf-Galois*

[*] Corresponding author

Email addresses: akoch@agnesscott.edu (Alan Koch), tkohl@math.bu.edu (Timothy Kohl), P.J.Truman@Keele.ac.uk (Paul J. Truman), runderwo@aum.edu (Robert Underwood)

structure on L/K, if L is an H-module algebra and the obvious K-linear map $L \otimes_K H \rightarrow \mathrm{End}_K(L)$ is bijective. For example, if L/K is a Galois extension with Galois group G then the group algebra $K[G]$, with action induced from the usual action of G on L, gives a Hopf-Galois structure on L/K. It is possible for two distinct Hopf-Galois structures on L/K to have underlying Hopf algebras which are isomorphic as K-Hopf algebras or as K-algebras; equivalently, one might view this as multiple actions of a single K-Hopf algebra or K-algebra on L. In this paper we study these phenomena.

If L/K is purely inseparable, it is known that a single Hopf algebra can act in an infinite number of ways: see e.g. [11]. We shall therefore suppose that L/K is separable. In this case Greither and Pareigis [10] have classified the Hopf-Galois structures admitted by L/K. In order to state this classification we require some notation. Let E be the Galois closure of L/K, $G = \mathrm{Gal}(E/K)$, and $G_L = \mathrm{Gal}(E/L)$. Let X denote the left coset space G/G_L, and define a homomorphism $\lambda : G \rightarrow \mathrm{Perm}(X)$ by $\lambda(\sigma)(\overline{\tau}) = \overline{\sigma\tau}$, where $\overline{\tau}$ denotes the coset $\tau G_L \in X$. The theorem of Greither and Pareigis asserts that there is a bijection between Hopf-Galois structures on L/K and subgroups N of $\mathrm{Perm}(X)$ which are regular (that is, having the same size as X and acting transitively on X) and normalized by $\lambda(G)$ (that is, stable under the action of G on $\mathrm{Perm}(X)$ defined by $\sigma * \eta = \lambda(\sigma)\eta\lambda(\sigma)^{-1}$). The enumeration of the Hopf-Galois structures admitted by L/K is therefore equivalent to the enumeration of subgroups of $\mathrm{Perm}(X)$ with these properties. If $|X|$ is large then this is a difficult problem, but in [2] Byott proved a "translation theorem", which provides a useful simplification. Loosely, for each abstract group N of order $|X|$, Byott's theorem relates the number of G-stable regular subgroups of $\mathrm{Perm}(X)$ that are isomorphic to N to the number of subgroups of the holomorph of N that are isomorphic to G. Since $\mathrm{Hol}(N) \cong N \rtimes \mathrm{Aut}(N)$, this group is much smaller than $\mathrm{Perm}(X)$. We give a more precise statement of Byott's theorem in subsection 2.2 below.

The theorem of Greither and Pareigis also asserts that the Hopf algebra appearing in the Hopf-Galois structure corresponding to the G-stable regular subgroup N of $\mathrm{Perm}(X)$ is $E[N]^G$, the fixed points of the group algebra $E[N]$ under the simultaneous action of G on E as Galois automorphisms and on N by the action $*$. We will refer to the isomorphism class of N as the *type* of Hopf-Galois structure given by $E[N]^G$. Now suppose that N_1, N_2 are G-stable regular subgroups of $\mathrm{Perm}(X)$, so that $H_1 = E[N_1]^G$ and $H_2 = E[N_2]^G$

are two Hopf algebras giving Hopf-Galois structures on L/K. It is well known (see, for example, [7] and [9]) that $H_1 \cong H_2$ as K-Hopf algebras if and only if there is an isomorphism $N_1 \xrightarrow{\sim} N_2$ that respects the action of G on each of these groups. In section 2 we state a slightly more general version of this result (Theorem 2.2), and provide a variety of examples. We show that it is possible to detect K-Hopf algebra isomorphisms by studying properties of their associated holomorphs (Theorem 2.11), and also determine a criterion for $F \otimes_K H_1$ and $F \otimes_K H_2$ to be isomorphic as F-Hopf algebras, for F some extension of K contained in E.

In section 3 we assume that K has characteristic zero and that H_1 and H_2 are commutative (equivalently, that N_1, N_2 are abelian groups). We determine a criterion, in terms of the dual groups $\widehat{N_1}$ and $\widehat{N_2}$, for $H_1 \cong H_2$ as K-algebras (Theorem 3.1). If $N_1 \cong N_2$, we show that it is also possible to detect such isomorphisms by studying properties of their associated holomorphs (Theorem 3.5). We show that these results have a particularly simple form in the case that N_1 and N_2 are both cyclic (Corollary 3.6). Finally, in section 4 we apply the results of the preceding sections to give a detailed analysis of the Hopf-Galois structures admitted by a cyclic extension L/K of odd prime power degree. We show that the Hopf algebras that appear are pairwise nonisomorphic as Hopf algebras (Theorem 4.1), and determine the K-algebra isomorphism classes (Theorem 4.10).

The authors would like to thank Prof. Griff Elder (University of Nebraska at Omaha) for organizing the annual conference “Hopf algebras and Galois module theory”, which enabled this collaboration to take place; as well as the University of Nebraska at Omaha for its hospitality. We are also grateful to the referee for his/her comments on this paper, and for the suggestion that we investigate possible generalizations of Corollary 3.6, which led to Example 4.12.

2. Hopf Algebra Isomorphisms

In this section we address the question of when two Hopf algebras giving Hopf-Galois structures on a finite separable extension of fields are isomorphic as Hopf algebras. Rather than focusing specifically on this situation, we make our definitions in more general terms:

Definition 2.1. *Let G be a group and let $(N_1, *_1), (N_2, *_2)$ be G-sets (where, for $i = 1, 2$, $*_i$ denotes the action of G on N_i). We say that $(N_1, *_1), (N_2, *_2)$ (or just N_1, N_2) are* isomorphic as G-sets *if there is a G-equivariant bijection $f : N_1 \to N_2$. We say that a G-set N is a* G-group *if it is a group on which G acts via automorphisms, and that two G-groups N_1, N_2 are* isomorphic as G-groups *if there is a G-equivariant group isomorphism $f : N_1 \xrightarrow{\sim} N_2$.*

Our main tool in this section will be the following well known theorem. We include a proof for the reader's convenience.

Theorem 2.2. *Let E/K be a Galois extension of fields, let G be a subgroup of Gal(E/K), and let $F = E^G$. Let $(N_1, *_1)$ and $(N_2, *_2)$ be G-groups and, for $i = 1, 2$, let G act on $E[N_i]$ by acting on E as Galois automorphisms and on N_i via $*_i$. Then $E[N_1]^G \cong E[N_2]^G$ as F-Hopf algebras if and only if $N_1 \cong N_2$ as G-groups.*

Proof. For $i = 1, 2$ let $\left(E[N_i]^G\right)^*$ denote the F-linear dual of $E[N_i]^G$. We show that $\left(E[N_1]^G\right)^* \cong \left(E[N_2]^G\right)^*$ as F-Hopf algebras if and only if there is a G-equivariant isomorphism $N_1 \xrightarrow{\sim} N_2$. For each i, $\left(E[N_i]^G\right)^*$ is a separable Hopf algebra, and therefore represents a finite étale group scheme $\mathcal{N}_i$, which corresponds to a finite group on which $\Gamma = \mathrm{Gal}(F^{\mathrm{sep}}/F)$ acts continuously [15, 6.3]. Explicitly, the corresponding group is

$$\begin{aligned} \mathcal{N}_i(F^{\mathrm{sep}}) &= \mathrm{Hom}_{F-alg}\left(\left(E[N_i]^G\right)^*, F^{\mathrm{sep}}\right) \\ &\cong \mathrm{Hom}_{F^{\mathrm{sep}}-alg}\left(F^{\mathrm{sep}} \otimes_F \left(E[N_i]^G\right)^*, F^{\mathrm{sep}}\right) \\ &\cong \mathrm{Hom}_{F^{\mathrm{sep}}-alg}(F^{\mathrm{sep}}[N_i]^*, F^{\mathrm{sep}}), \end{aligned}$$

with Γ acting via its action on F^{sep}. This group is isomorphic to N_i, and the action of Γ factors through the original action of G on N_i. Therefore $\left(E[N_1]^G\right)^* \cong \left(E[N_2]^G\right)^*$ as F-Hopf algebras if and only if there is a G-equivariant isomorphism $N_1 \xrightarrow{\sim} N_2$. □

Now recall the notation established in section 1 to describe the theorem of Greither and Pareigis: L/K is a finite separable extension of fields with Galois closure E, $G = \mathrm{Gal}(E/K)$, $G_L = \mathrm{Gal}(E/L)$, $X = G/G_L$. A Hopf algebra giving a Hopf-Galois structure on L/K then has the form $E[N]^G$ for some regular subgroup N of Perm(X) stable under the action of G on Perm(X) by $\sigma * \eta = \lambda(\sigma)\eta\lambda(\sigma)^{-1}$. We have:

Corollary 2.3. *Let $E[N_1]^G$ and $E[N_2]^G$ give Hopf-Galois structures on L/K. Then $E[N_1]^G \cong E[N_2]^G$ as K-Hopf algebras if and only if $N_1 \cong N_2$ as G-groups.*

We illustrate the applicability of the theory with a variety of examples.

Example 2.4. (The classical and canonical nonclassical Hopf-Galois structures) If L/K is a Galois extension then in the notation of the theorem of Greither and Pareigis we have $E = L$, $G_L = \{1\}$, and $X = G$, and the homomorphism $\lambda : G \to \mathrm{Perm}(G)$ is in fact the left regular embedding of G. In this case examples of G-stable regular subgroups of $\mathrm{Perm}(G)$ are $\lambda(G)$ itself and $\rho(G)$, the image of G under the right regular embedding (these subgroups coincide if and only if G is abelian). The elements of $\rho(G)$ commute with those of $\lambda(G)$, so the action of G on $\rho(G)$ is trivial, and therefore the Hopf algebra appearing in the Hopf-Galois structure corresponding to $\rho(G)$ is $L[\rho(G)]^G = L^G[\rho(G)] = K[\rho(G)]$, which is isomorphic to the Hopf algebra $K[G]$. We call this the *classical Hopf-Galois structure* on L/K. If G is nonabelian then the subgroup $\lambda(G)$ corresponds to a different Hopf-Galois structure on L/K, which we call the *canonical nonclassical Hopf-Galois structure.* The Hopf algebra appearing in this structure is $H_\lambda := L[\lambda(G)]^G$. Since G is nonabelian the action of G on $\lambda(G)$ is not trivial (the orbits are the conjugacy classes in $\lambda(G)$), and so $\rho(G) \not\cong \lambda(G)$ as G-groups in this case. Therefore, by Corollary 2.3, $K[G] \not\cong H_\lambda$ as K-Hopf algebras.

Example 2.5. (Elementary abelian extensions of degree p^2) Let $p > 2$ be prime, and let L/K be a Galois extension of fields of degree p^2 with elementary abelian Galois group G. In [2, Corollary to Theorem 1, part (iii)] it is shown that L/K admits p^2 Hopf-Galois structures. By applying Corollary 2.3 we can determine which of these Hopf-Galois structures involve isomorphic Hopf algebras. In [3, Theorem 2.5] the regular subgroups of $\mathrm{Perm}(G)$ that yield the Hopf-Galois structures are determined as follows: let T be a subgroup of G of order p, and fix elements $s, t \in G$ such that

$$T = \langle t \rangle, \quad s^p = 1_G, \quad G = \langle s, t \rangle.$$

Let $d \in \{0, 1, \ldots, p-1\}$, and define $\alpha, \beta \in \mathrm{Perm}(G)$ in terms of their actions on a typical element $s^k t^l \in G$:

$$\begin{aligned} \alpha[s^k t^l] &= s^k t^{l-1} \\ \beta[s^k t^l] &= s^{k-1} t^{l+(k-1)d}. \end{aligned} \tag{1}$$

It is easily verified that $\alpha^p = \beta^p = 1$ and $\alpha\beta = \beta\alpha$, whence $N_{T,d} = \langle \alpha, \beta \rangle \cong G$. Moreover, one can show that $N_{T,d}$ is a regular subgroup of $\mathrm{Perm}(G)$, and that

$$s * \alpha = \alpha, \quad t * \alpha = \alpha, \quad s * \beta = \alpha^d \beta, \quad t * \beta = \beta. \tag{2}$$

Thus $N_{T,d}$ is G-stable, and therefore corresponds to a Hopf-Galois structure on L/K with Hopf algebra $H_{T,d} = L[N_{T,d}]^G$. If $d = 0$ then $N_{T,d} = \rho(G)$ regardless of the choice of T, and so we obtain the classical Hopf-Galois structure. Taking $1 \leq d \leq p-1$ and letting T vary through the subgroups of G of order p, we obtain $p^2 - 1$ distinct groups $N_{T,d} \neq \rho(G)$, giving in total p^2 Hopf-Galois structures on L/K. These are all the Hopf-Galois structures on L/K.

We claim that two Hopf algebras $H_1 = H_{T_1,d_1}$ and $H_2 = H_{T_2,d_2}$ are isomorphic as Hopf algebras if and only if $d_1 = d_2 = 0$ or $d_1 d_2 \neq 0$ and $T_1 = T_2$. Let

$$\begin{array}{rclcl} N_1 & = & N_{T_1,d_1} & = & \langle \alpha_1, \beta_1 \rangle \\ N_2 & = & N_{T_2,d_2} & = & \langle \alpha_2, \beta_2 \rangle, \end{array}$$

where α_1, β_1 and α_2, β_2 are defined as α, β are in Equations (1), using d_1, d_2 as appropriate. We have seen that if $d_1 = d_2 = 0$ then $H_1 = H_2$. If $d_1 d_2 \neq 0$ and $T_1 = T_2$ then there exists $c \in \{1, \ldots, p-1\}$ such that $cd_2 \equiv d_1 \pmod{p}$. Using this, define a homomorphism $\varphi : N_1 \to N_2$ by

$$\varphi(\alpha_1) = \alpha_2, \quad \varphi(\beta_1) = \beta_2^c.$$

It is clear that φ is an isomorphism, and we claim that it is G-equivariant. We have:

$$\begin{array}{l} \varphi(s * \alpha_1) = \varphi(\alpha_1) = \alpha_2 = s * \alpha_2 = s * \varphi(\alpha_1), \\ \varphi(t * \alpha_1) = \varphi(\alpha_1) = \alpha_2 = t * \alpha_2 = t * \varphi(\alpha_1), \\ \varphi(s * \beta_1) = \varphi(\alpha_1^{d_1} \beta_1) = \alpha_2^{d_1} \beta_2^c = \alpha_2^{d_2 c} \beta_2^c = s * \beta_2^c = s * \varphi(\beta_1), \\ \varphi(t * \beta_1) = \varphi(\beta_1) = \beta_2^c = t * \beta_2^c = t * \varphi(\beta_1). \end{array}$$

Thus φ is a G-equivariant isomorphism of N_1 onto N_2, and so $H_1 \cong H_2$ as Hopf algebras by Corollary 2.3.

For the converse, note that if T is a subgroup of G of order p and $d \neq 0$ then by (2) the kernel of the action of G on $N_{T,d}$ is precisely T. Therefore, if $d_1 d_2 \neq 0$ and $N_1 \cong N_2$ as G-groups then we must have $T_1 = T_2$.

Thus, the p^2 Hopf-Galois structures admitted by L/K involve exactly $p+2$ nonisomorphic Hopf algebras: the group algebra $K[G]$ with its usual action on L and, for each of the $p+1$ subgroups T of G of order p, a Hopf algebra $H_T = H_{T,1}$, acting in $p-1$ different ways.

Example 2.6. (Fixed point free endomorphisms) If L/K is a finite Galois extension of fields with nonabelian Galois group G then, as described above, L/K admits a canonical nonclassical Hopf-Galois structure with Hopf algebra $H_\lambda = L[\lambda(G)]^G$. In [7], Childs shows how certain endomorphisms of G can yield further Hopf-Galois structures on L/K, whose Hopf algebras are isomorphic to H_λ. Specifically, let ψ be an endomorphism of G which is abelian (meaning $\psi(gh) = \psi(hg)$ for all $g, h \in G$) and fixed point free (meaning $\psi(g) = g$ if and only if $g = 1_G$). From ψ we may construct a homomorphism $\alpha_\psi : G \to \mathrm{Perm}(G)$ defined by

$$\alpha_\psi(g) = \lambda(g)\rho(\psi(g)).$$

One can show that $\alpha_\psi(G)$ is a G-stable regular subgroup of $\mathrm{Perm}(G)$, which therefore corresponds to a Hopf-Galois structure on L/K. It is shown in [7, Theorem 5] that the Hopf algebras appearing in the Hopf-Galois structures produced by this construction are all isomorphic to H_λ as Hopf algebras. A similar approach appears in [8]; in particular [8, Corollary 8.3] calculates the precise number of Hopf-Galois actions of H_λ on a Galois extension whose Galois group is a semidirect product of certain cyclic groups. We can reinterpret these ideas via Corollary 2.3: $\lambda(G)$ and $\alpha_\psi(G)$ are both regular subgroups of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$, and it is easy to verify that the map $\varphi : \lambda(G) \to \alpha_\psi(G)$ defined by

$$\varphi(\lambda(g)) = \alpha_\psi(g) = \lambda(g)\rho(\psi(g)).$$

is a G-equivariant isomorphism of groups. Therefore $L[\alpha_\psi(G)]^G \cong L[\lambda(G)]^G$ as Hopf algebras.

Example 2.7. (Conjugating regular subgroups by elements of $\rho(G)$) Let L/K be a Galois extension of fields with nonabelian Galois group G, and let $L[N]^G$ give a Hopf-Galois structure on L/K. Since G is nonabelian, we have $\lambda(G) \neq \rho(G)$ and so, although N is normalized by $\lambda(G)$, it may not be normalized by $\rho(G)$. For $g \in G$, let $N_g = \rho(g)N\rho(g)^{-1} \neq N$. Then N_g is a regular subgroup of Perm(G) since N is regular, and the group isomorphism $\varphi : N \to N_g$ defined by

$$\varphi(\eta) = \rho(g)\eta\rho(g)^{-1}$$

is easily shown to be G-equivariant. Therefore N_g is G-stable, and so corresponds to a Hopf-Galois structure on L/K, with Hopf algebra $L[N_g]^G$. Moreover, by Corollary 2.3 we have $L[N_g]^G \cong L[N]^G$ as Hopf algebras.

Example 2.8. (A specific example of conjugating by elements of $\rho(G)$)
Let p, q be primes with $p \equiv 1 \pmod{q}$, and let L/K be a Galois extension of fields with group isomorphic to the metacyclic group of order pq:

$$G = \langle \sigma, \tau \mid \sigma^p = \tau^q = 1,\ \tau\sigma = \sigma^g\tau \rangle,$$

where g is a fixed positive integer whose order modulo p is q. By [4, Theorem 6.2], L/K admits precisely $2 + p(2q - 3)$ Hopf-Galois structures, of which precisely p have cyclic type. We can use Example 2.7 to show that the Hopf algebras appearing in the Hopf-Galois structures of cyclic type are all isomorphic as Hopf algebras. The corresponding regular subgroups N_c ($c = 0, \ldots, p-1$) of Perm(G) are described explicitly in [4, Lemma 4.1], each in terms of two generators. Using these descriptions, we can verify that $N_c = \langle \eta_c \rangle$, where

$$\eta_c = \lambda(\sigma)\rho(\sigma^{-c}\tau)^{-1}.$$

Using the fact that $\lambda(G)$ and $\rho(G)$ commute inside Perm(G) we have in particular

$$\rho(\sigma^i)\eta_0\rho(\sigma^{-i}) = \eta_{i(g-1)},$$

where the subscript should be interpreted modulo p. Since g has order q modulo p we certainly have $g - 1 \not\equiv 0 \pmod{p}$ and so, given $c = 0, \ldots, p-1$ there exists i such that

$$\rho(\sigma^i)\eta_0\rho(\sigma^{-i}) = \eta_c.$$

Therefore the groups N_c are all isomorphic as G-groups, and so the Hopf algebras H_c are all isomorphic as K-Hopf algebras.

In the case that $q = 2$ (so that $G \cong D_p$, the dihedral group of order $2p$), this result is established in [12, Section 4, Proposition 3], by methods different to those employed above.

2.1. Hopf algebra isomorphisms after base change

We return to the situation addressed by the theorem of Greither and Pareigis, as described in section 1. Suppose that $E[N_1]^G$ and $E[N_2]^G$ are two Hopf algebras giving Hopf-Galois structure on L/K, and that $N_1 \cong N_2$. Then $E \otimes_K E[N_i]^G = E[N_i]$ for each i, so certainly $E \otimes_K E[N_1]^G \cong E \otimes_K E[N_2]^G$ as E-Hopf algebras. However, there may exist intermediate fields K' such that $K' \otimes_K E[N_1]^G \cong K' \otimes_K E[N_2]^G$ as K'-Hopf algebras. We may use Theorem 2.2 to detect Galois extensions K' of K with this property. In this case, let $G' = \mathrm{Gal}(E/K')$; then for $i = 1, 2$ we have

$$E[N_i]^G = \left(E[N_i]^{G'}\right)^{G/G'}$$

and

$$K' \otimes_K \left(E[N_i]^{G'}\right)^{G/G'} = E[N_i]^{G'}.$$

Therefore

$$K' \otimes_K E[N_i]^G = E[N_i]^{G'}$$

for $i = 1, 2$, and so $K' \otimes_K E[N_1]^G \cong K' \otimes_K E[N_2]^G$ as K'-Hopf algebras if and only if $E[N_1]^{G'} \cong E[N_2]^{G'}$ as K'-Hopf algebras. By Theorem 2.2 this occurs if and only if $(N_1, *) \cong (N_2, *)$ as G'-groups.

Example 2.9. (The smallest extension of scalars giving a group algebra) Let $E[N]^G$ be a Hopf algebra giving a Hopf-Galois structure on L/K, and let G' denote the kernel of the action of G on N. Then $E[N]^{G'} = E^{G'}[N] = K'[N]$, a group algebra with coefficients drawn from the field $E^{G'} = K'$. Therefore we have $K' \otimes_K E[N]^G = K'[N]$. In fact K' is minimal amongst the subfields F of E such that $F \otimes_K E[N]^G$ is isomorphic as a Hopf algebra to a group algebra (see [10, Corollary 3.2]).

Example 2.10. (Elementary abelian extensions of degree p^2 revisited) Let p be an odd prime, and let L/K be an elementary abelian extension of degree p^2 with group G. In Example 2.5 we determined which of the Hopf algebras appearing in the classification of Hopf-Galois structures on L/K are isomorphic as K-Hopf algebras. Here we can show that, given any two Hopf algebras H_1, H_2 giving nonclassical Hopf-Galois structures on the extension, there exists a subfield K' of L/K of degree p over K such that $K' \otimes_K H_1 \cong K' \otimes_K H_2$ as K'-Hopf algebras. Recall from Example 2.5 that for $i = 1, 2$ the Hopf algebra H_i corresponds to a choice of subgroup T_i of degree p and an integer $d_i \in \{1, \dots, p-1\}$ (the possibility $d_i = 0$ is excluded since the Hopf algebras give nonclassical structures). Specifically, we have $H_i = L[N_i]^G$, where N_i is generated by two permutations α_i, β_i as described in Equations (1) and the action of G on N_i is as described in Equation (2). From this last equation, we see that the kernel of the action of G on each N_i is precisely T_i, which we now write as $\langle t_i \rangle$. Let $g' = t_1 t_2$, $G' = \langle g' \rangle$, and $K' = L^{G'}$. For each i we have $g' * \alpha_i = \alpha_i$ for each i. The action of g' on the β_i is:

$$g' * \beta_1 = t_1 t_2 * \beta_1 = t_2 * \beta_1 = \alpha_1^{u_1} \beta_1 \text{ for some } u_1 \in \{1, \dots, p-1\}$$

and

$$g' * \beta_2 = t_1 t_2 * \beta_2 = t_1 * \beta_2 = \alpha_2^{u_2} \beta_2 \text{ for some } u_2 \in \{1, \dots, p-1\}.$$

Let c be an integer such that $cu_2 \equiv u_1 \pmod{p}$; then the map $\varphi : N_1 \to N_2$ defined by

$$\varphi(\alpha_1) = \alpha_2, \quad \varphi(\beta_1) = \beta_2^c$$

is clearly an isomorphism, and is easily shown to be G'-equivariant. Therefore we have

$$K' \otimes_K H_1 \cong K' \otimes_K H_2 \text{ as } K'\text{-Hopf algebras.}$$

2.2. Hopf algebra isomorphisms via the holomorph

We retain the notation of subsection 2.1, but now view N_1, N_2 as images of a single abstract group N under embeddings $\alpha_1, \alpha_2 : N \hookrightarrow \mathrm{Perm}(X)$. Byott's translation theorem [2, Proposition 1] relates such embeddings to certain embeddings of G into the holomorph of N, denoted $\mathrm{Hol}(N)$, which is normalizer of $\lambda(N)$ inside $\mathrm{Perm}(N)$. More precisely, there is a bijection between the sets

$$\{\alpha : N \hookrightarrow \mathrm{Perm}(X) \mid \alpha(N) \text{ is } G\text{-stable and regular}\}$$

and

$$\{\beta : G \hookrightarrow \mathrm{Hol}(N) \mid \beta(G_L) \text{ is the stabilizer of } e_N\}.$$

Of course, different embeddings α can have the same image (and so correspond to the same Hopf-Galois structure), but this can be detected by studying the corresponding β: we have $\alpha_1(N) = \alpha_2(N)$ if and only if there exists $\mu \in \mathrm{Aut}(N)$ such that $\beta_2(g) = \mu \beta_1(g) \mu^{-1}$ for all $g \in G$. In fact, we can also detect when the Hopf-Galois structures corresponding to different embeddings α_1, α_2 involve isomorphic Hopf algebras by studying properties of the corresponding β_1, β_2:

Theorem 2.11. *Let α_1, α_2 be embeddings of N into Perm(X) whose images are regular and normalized by $\lambda(G)$, and let β_1, β_2 be the corresponding embeddings of G into Hol(N). Viewing Hol(N) as $\rho(N) \rtimes$ Aut(N), let $\overline{\beta_1}, \overline{\beta_2}$ denote the compositions of β_1, β_2 with the projection onto the automorphism component. Then*

$$E[\alpha_1(N)]^G \cong E[\alpha_2(N)]^G \text{ as Hopf algebras}$$

if and only if there exists $\mu \in$ Aut(N) such that

$$\overline{\beta_2}(g) = \mu\overline{\beta_1}(g)\mu^{-1} \text{ for all } g \in G.$$

Proof. By Theorem 2.2, we have $E[\alpha_1(N)]^G \cong E[\alpha_2(N)]^G$ as Hopf algebras if and only if $(\alpha_1(N), *) \cong (\alpha_2(N), *)$ as G-groups. For $i = 1, 2$ define an action $*_i$ of G on N by $g *_i \eta = \overline{\beta_i}(g)[\eta]$; then by [5, (7.7) Proposition] we have that $(\alpha_i(N), *) \cong (N, *_i)$ as G-groups, and so $(\alpha_1(N), *) \cong (\alpha_2(N), *)$ as G-groups if and only if $(N, *_1) \cong (N, *_2)$ as G-groups. This occurs if and only if there exists $\mu \in \mathrm{Aut}(N)$ such that

$$\mu(g *_1 \eta) = g *_2 \mu(\eta) \text{ for all } g \in G, \eta \in N,$$

that is, if and only if

$$\mu\overline{\beta_1}(g) = \overline{\beta_2}(g)\mu \text{ for all } g \in G.$$

□

As a special case, we have

Corollary 2.12. *If Aut(N) is abelian (in particular, if N is cyclic), then $E[\alpha_1(N)]^G \cong E[\alpha_2(N)]^G$ as Hopf algebras if and only if $\overline{\beta_1}(g) = \overline{\beta_2}(g)$ for all $g \in G$.*

Example 2.13. (The classical and canonical nonclassical Hopf-Galois structures revisited) Recall Example 2.4, and assume that G is nonabelian. In the notation of this subsection, we may take $N = G$ and view λ and ρ as embeddings of the abstract group G into Perm(G) whose images are G-stable and regular. By following the details of the proof of Byott's translation theorem, we find that the embedding $G \hookrightarrow \mathrm{Hol}(G)$ corresponding to ρ is ρ itself, and similarly for λ. When we view Hol(G) as $\rho(G) \rtimes \mathrm{Aut}(G)$, we have $\rho(G) = \{(\rho(g), 1) \mid g \in G\}$, whereas $\lambda(G) = \{(\rho(g^{-1}), c(g)) \mid g \in G\}$, where $c(g)$ is the inner automorphism of G arising from conjugation by g. Therefore $\overline{\rho}(G)$ and $\overline{\lambda}(G)$ have different orders, and so there cannot exist an automorphism $\mu \in \mathrm{Aut}(G)$ with the properties required by Theorem 2.11. Hence we recover the fact that $K[G] \ncong H_\lambda$ as K-Hopf algebras.

3. Algebra Isomorphisms for Commutative Structures

Let E/K be a Galois extension of fields with Galois group G, and let $(N_1, *_1)$ and $(N_2, *_2)$ be G-groups. In this section, we consider the question of when the Hopf algebras $E[N_1]^G$ and $E[N_2]^G$ are isomorphic as K-algebras. We shall assume that $E[N_1]^G$ and $E[N_2]^G$ are commutative algebras; this is equivalent to assuming that the underlying groups N_1, N_2 are abelian. Note, however, that we do not assume that these groups are isomorphic, nor that G is abelian. We shall also assume that K has characteristic zero; a consequence of this is that each $E[N_i]^G$ is a separable K-algebra and is thus isomorphic as a K-algebra to a product of extension fields of K.

Let K^{sep} denote a separable closure of K, and let $\Gamma = \mathrm{Gal}(K^{\mathrm{sep}}/K)$. For $i = 1, 2$ let Γ act on $K^{\mathrm{sep}}[N_i]$ by acting on K^{sep} as Galois automorphisms and on N_i by factoring through G. Then $K^{\mathrm{sep}}[N_i]^\Gamma = E[N_i]^G$. The action of Γ on N_i induces an action of Γ on the dual group $\widehat{N_i}$ by $(\gamma *_i \chi)[\eta] = \gamma(\chi[\gamma^{-1} *_i \eta])$ for all $\eta \in N_i$.

Theorem 3.1. *We have $E[N_1]^G \cong E[N_2]^G$ as K-algebras if and only if $\widehat{N_1} \cong \widehat{N_2}$ as Γ-sets.*

Proof. We show that $K^{\mathrm{sep}}[N_1]^\Gamma \cong K^{\mathrm{sep}}[N_2]^\Gamma$ as K-algebras if and only if $\widehat{N_1} \cong \widehat{N_2}$ as Γ-sets, using the correspondence between separable K-algebras and finite sets on which Γ acts continuously [15, 6.3]. As in the proof of Theorem 2.2, for $i = 1, 2$, let $\mathcal{N}_i$ be the finite étale group scheme represented by H_i^*, with corresponding Γ-group N_i. Then the Cartier dual $\mathcal{N}_i^D$ is represented by H_i, and the corresponding Γ-set is

$$\mathcal{N}_i^D(K^{\mathrm{sep}}) = \mathrm{Hom}_{K^{\mathrm{sep}}-grp}(\mathcal{N}_{i,K^{\mathrm{sep}}}, \mathbb{G}_{m,K^{\mathrm{sep}}}),$$

which corresponds naturally to the set of grouplike elements of $K^{\mathrm{sep}} \otimes_K H_i^*$. Since N_i is abelian we have

$$K^{\mathrm{sep}} \otimes_K H_i^* = K^{\mathrm{sep}}[N_i]^* = K^{\mathrm{sep}}[\widehat{N_i}],$$

and so $\mathcal{N}_i^D(K^{\mathrm{sep}}) = \widehat{N_i}$, with Γ acting as described above. Therefore $H_1 \cong H_2$ as K-algebras if and only if $\widehat{N_1} \cong \widehat{N_2}$ as Γ-sets.

□

The following corollary is the principal application of Theorem 3.1.

Corollary 3.2. *Let $E[N_1]^G$ and $E[N_2]^G$ be commutative Hopf algebras giving Hopf-Galois structures on a finite separable extension of fields L/K. Then $E[N_1]^G \cong E[N_2]^G$ as K-algebras if and only if $\widehat{N_1} \cong \widehat{N_2}$ as Γ-sets.*

Example 3.3. (Elementary abelian extensions of degree p^2 revisited) Let p be an odd prime and let L/K be an elementary abelian extension of degree p^2 with group G. In Example 2.5 we determined criteria for two Hopf algebras H_1, H_2 giving Hopf-Galois structures on L/K to be isomorphic as K-Hopf algebras. Under the additional hypotheses that K has characteristic zero and contains a primitive p^{th} root of unity ζ, we now apply Corollary 3.2 to determine criteria for them to be isomorphic as K-algebras. In fact, we show that in this case $H_1 \cong H_2$ as K-algebras if and only if $H_1 \cong H_2$ as K-Hopf algebras.

Recall from Example 2.5 a Hopf algebra H giving a Hopf-Galois structures on L/K determined by a choice of subgroup T of degree p and an integer $d \in \{0, \ldots, p-1\}$; the Hopf algebra is then $L[N]^G$, where N is the subgroup of $\mathrm{Perm}(G)$ generated by two permutations α, β as described in Equations (1), and the action of G on N is as described in Equation (2). The dual group $\widehat{N}$ is therefore generated by two characters χ, ψ, defined as follows:

$$\chi(\alpha) = \zeta, \quad \chi(\beta) = 1, \quad \psi(\alpha) = 1, \quad \psi(\beta) = \zeta.$$

Since L/K is a Galois extension the action of G on N described in Equation (2) translates into an action of G on $\widehat{N}$ by

$$s * \chi = \chi\psi^{-d}, \quad t * \chi = \chi, \quad s * \psi = \psi, \quad t * \psi = \psi, \tag{3}$$

where $-d$ is to be interpreted modulo p. Now let H_1, H_2 be two such Hopf algebras giving distinct Hopf-Galois structures on L/K, with underlying groups N_1, N_2 as in Example 2.5. We claim that $H_1 \cong H_2$ as K-algebras if and only if $d_1 = d_2 = 0$ or $d_1 d_2 \neq 0$ and $T_1 = T_2$; these are identical to the conditions we derived in Example 2.5 for $H_1 \cong H_2$ as K-Hopf algebras. If these conditions are satisfied then $H_1 \cong H_2$ as K-Hopf algebras, so certainly as K-algebras. For the converse, note that by (3) if $d_i = 0$ then G acts trivially on $\widehat{N_i}$, whereas if T is a subgroup of G of order p and $d \neq 0$ then the kernel of the action of G on $N_{T,d}$ is precisely T. Therefore if $\widehat{N_1} \cong \widehat{N_2}$ as G-sets then we must have $d_1 = d_2 = 0$ or $d_1 d_2 \neq 0$ and $T_1 = T_2$.

We remark that $H_i \cong K^p \times \left(L^{T_i}\right)^{p-1}$ as K-algebras: see [14, Proposition 3.4].

3.1. Algebra isomorphisms via the holomorph

Hitherto in this section we have not assumed that N_1, N_2 are isomorphic as groups; we now impose this assumption. We can therefore view N_1, N_2 as the images of a single abstract abelian group N under two embeddings $\alpha_1, \alpha_2 : N \hookrightarrow \mathrm{Perm}(X)$, as in subsection 2.2. We recall from that subsection that By Byott's translation theorem these embeddings correspond to embeddings $\beta_1, \beta_2 : G \hookrightarrow \mathrm{Hol}(N) = \rho(N) \rtimes \mathrm{Aut}(N)$, and we write $\overline{\beta_1}, \overline{\beta_2}$ for the compositions of β_1, β_2 with the projection onto the $\mathrm{Aut}(N)$ component. We have seen in Theorem 2.11 that it is possible to detect when $E[\alpha_1(N)]^G \cong E[\alpha_2(N)]^G$ as K-Hopf algebras by studying properties of $\overline{\beta_1}, \overline{\beta_2}$. We shall show that in our situation these maps also allow us to detect K-algebra isomorphisms.

As in the proof of Theorem 2.11, for $i = 1, 2$ define an action $*_i$ of G on N by $g *_i \eta = \overline{\beta_i}(g)[\eta]$; then by [5, (7.7)] we have that $(\alpha_i(N), *) \cong (N, *_i)$ as G-groups. We may extend these to actions of Γ by factoring through G, obtaining $(\alpha_i(N), *) \cong (N, *_i)$ as Γ-groups. Each of the actions of Γ on N yields a dual action of Γ on $\widehat{N}$, which we also denote by $*_i$. Similarly, the action of Γ on each $\alpha_i(N)$ yields a dual action $*$ of Γ on each $\widehat{\alpha_i(N)}$.

Lemma 3.4. *For $i = 1, 2$ we have $(\widehat{\alpha_i(N)}, *) \cong (\widehat{N}, *_i)$ as Γ-groups.*

Proof. For each $i = 1, 2$, the map $\alpha_i : (N, *_i) \to (\alpha_i(N), *)$ is a Γ-equivariant isomorphism. It is routine to verify that for each $\chi \in \widehat{N}$ the function $\psi_\chi : \alpha_i(N) \to K^{\mathrm{sep}}$ defined by $\psi_\chi[\alpha_i(\eta)] = \chi[\eta]$ for all $\eta \in N$ is a character of $\alpha_i(N)$, and that the map $\psi : \widehat{N} \to \widehat{\alpha_i(N)}$ defined by $\psi(\chi) = \psi_\chi$ is a Γ-equivariant isomorphism. □

Theorem 3.5. *We have $E[\alpha_1(N)]^G \cong E[\alpha_2(N)]^G$ as K-algebras if and only if $(\widehat{N}, *_1) \cong (\widehat{N}, *_2)$ as Γ-sets.*

Proof. By Theorem 3.1 we have $E[\alpha_1(N)]^\Gamma \cong E[\alpha_2(N)]^\Gamma$ as K-algebras if and only if $(\widehat{\alpha_1(N)}, *) \cong (\widehat{\alpha_2(N)}, *)$ as Γ-sets, and by Lemma 3.4 this occurs if and only if $(\widehat{N}, *_1) \cong (\widehat{N}, *_2)$ as Γ-sets. □

The following corollary shows that in certain cases we can detect K-algebra isomorphisms by working directly with N, rather than $\widehat{N}$. We shall exploit this in section 4, as part of our analysis of the Hopf algebras giving Hopf-Galois structures on a cyclic extension of odd prime power degree.

Corollary 3.6. *Suppose that N is cyclic and that K contains a primitive $|N|^{th}$ root of unity ζ. Then the following are equivalent:*

1. $E[\alpha_1(N)]^G \cong E[\alpha_2(N)]^G$ *as K-algebras;*
2. $(\widehat{\alpha_1(N)}, *) \cong (\widehat{\alpha_2(N)}, *)$ *as Γ-sets;*
3. $(\widehat{N}, *_1) \cong (\widehat{N}, *_2)$ *as Γ-sets;*
4. $(\alpha_1(N), *) \cong (\alpha_2(N), *)$ *as Γ-sets;*
5. $(N, *_1) \cong (N, *_2)$ *as Γ-sets.*

Proof. (1), (2), and (3) are equivalent by Theorem 3.1 and Theorem 3.5, and (4) and (5) are equivalent since for each i we have $(\alpha_i(N), *) \cong (N, *_i)$ as Γ-groups. We show that (3) is equivalent to (5).

Let η be a generator of N, and define $\chi : N \to K$ by $\chi(\eta) = \zeta$; then χ is a generator of $\widehat{N}$. We claim that for $i = 1, 2$, the isomorphism $f : N \to \widehat{N}$ defined by $f(\eta) = \chi$ has the property that

$$\gamma *_i f(\eta) = f(\gamma^{-1} *_i \eta).$$

To see this, note that each $\gamma \in \Gamma$ acts as an automorphism of N, so there exists an integer $e = e(i, \gamma)$ (coprime to $|N|$) such that $\gamma *_i \eta = \eta^e$. Now using the assumption that $\zeta \in K$, for all $\nu \in N$ we have:

$$(\gamma *_i f(\eta))[\nu] = \chi[\gamma^{-1} *_i \nu] = \chi[\nu^{e^{-1}}] = \chi^{e^{-1}}[\nu] = f(\gamma^{-1} *_i \eta)[\nu],$$

where e^{-1} is computed modulo $|N|$. It follows that the isomorphism f has the desired property. We therefore obtain a diagram:

$$\begin{tikzcd}
(N, *_1) \arrow[r, dashed, "\pi"] \arrow[d, "f"] & (N, *_2) \arrow[d, "f"] \\
(\widehat{N}, *_1) \arrow[r, dashed, "\widehat{\pi}"] & (\widehat{N}, *_2)
\end{tikzcd}$$

If π is a Γ-equivariant bijection, then $f \circ \pi \circ f^{-1}$ is a Γ equivariant bijection, and if $\widehat{\pi}$ is a Γ-equivariant bijection, then $f^{-1} \circ \widehat{\pi} \circ f$ is a Γ-equivariant bijection. □

We remark that parts (3) and (5) of Corollary 3.6 are not equivalent if K does not contain a primitive $|N|^{\text{th}}$ root of unity: see Example 4.12.

4. Cyclic Extensions of Prime Power Degree

Let p be an odd prime number and L/K a cyclic extension of degree p^n. By a result of Kohl [13, Theorem 3.3] (see also [5, (9.1)]), there are precisely p^{n-1} Hopf-Galois structures on L/K, and they all have cyclic type. Explicit K-algebra generators for the Hopf algebras appearing in these Hopf-Galois structures were determined in [6, §6.3], requiring intricate manipulations. In this section we apply to results of section 2 and 3 to determine which of the Hopf algebras appearing in these Hopf-Galois structures are isomorphic as K-Hopf algebras or K-algebras, and (in the case that K has characteristic zero and contains a primitive p^n-th root of unity) explicitly determine their Wedderburn-Artin decompositions.

Since the Hopf-Galois structures admitted by L/K all have cyclic type, we can view the corresponding regular subgroups of $\text{Perm}(G)$ as images of a single abstract cyclic group $N = \langle \eta \rangle$ of order p^n under p^{n-1} different embeddings $\alpha_s : N \hookrightarrow \text{Perm}(G)$. By Byott's translation, each such α_s corresponds to an embedding $\beta_s : G \to \text{Hol}(N)$, and these are described in [5, (8.6) and (9.1)]: let $G = \langle \sigma \rangle$, and let δ be the $(p-1)^{st}$ power of some generator of the cyclic group $\text{Aut}(N)$. Then the embeddings we seek are of the form $\beta_s : G \hookrightarrow \text{Hol}(N)$ with

$$\beta_s(\sigma) = (\rho(\eta), \delta^s), 0 \leq s < p^{n-1}.$$

For each s, let $\alpha_s : N \hookrightarrow \text{Perm}(G)$ denote the embedding corresponding to β_s, and let $H_s = L[\alpha_s(N)]^G$ denote the corresponding Hopf algebra.

Theorem 4.1. *Let $0 < r, s \leq p^{n-1}$. Then $H_r \cong H_s$ as K-Hopf algebras if and only if $r = s$.*

Proof. Since N is cyclic, $\text{Aut}(N)$ is abelian, and so by Corollary 2.12 we have $H_r \cong H_s$ as K-Hopf algebras if and only if $\overline{\beta_r}(g) = \overline{\beta_s}(g)$ for all $g \in G$. Since in this case G is generated by σ, this occurs if and only if $\overline{\beta_r}(\sigma) = \overline{\beta_s}(\sigma)$; that is, if and only if $\delta^r = \delta^s$. Hence $H_r \cong H_s$ as K-Hopf algebras if and only if $r = s$. □

Therefore the Hopf algebras giving the Hopf-Galois structures on L/K are pairwise nonisomorphic. We can determine which of them become isomorphic under various base changes. Let

$$K = K_0 \subset K_1 \subset \cdots \subset K_n = L$$

be the maximal tower of field extensions, and for each $i = 0, \ldots, n$ let $G_i = \langle \sigma^{p^i} \rangle = \mathrm{Gal}(L/K_i)$.

Theorem 4.2. *For $0 < r, s \leq p^{n-1}$ and $0 \leq i \leq n-1$, we have $K_i \otimes_K H_r \cong K_i \otimes_K H_s$ as K_i-Hopf algebras if and only if $r \equiv s \pmod{p^{n-1-i}}$.*

Proof. By Theorem 2.2, we have $K_i \otimes_K H_r \cong K_i \otimes_K H_s$ as K_i-Hopf algebras if and only if $(\alpha_r(N), *) \cong (\alpha_s(N), *)$ as G_i-groups. By [5, (7.7)], this is equivalent to $(N, *_r) \cong (N, *_s)$ as G_i-groups, so we must show that this occurs if and only if $r \equiv s \pmod{p^{n-1-i}}$.

Recall that $\delta \in \mathrm{Aut}(N)$ has order p^{n-1}, so there exists an element $d \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ of order p^{n-1} such that $\delta(\eta) = \eta^d$. It follows that for $0 \leq j \leq p^n - 1$ we have

$$\sigma^j *_r \eta = \overline{\beta_r}(\sigma)^j[\eta] = \delta^{rj}\eta = \eta^{d^{rj}},$$

and similarly $\sigma^j *_s \eta = \eta^{d^{sj}}$. Now let θ be an automorphism of N, and write $\theta(\eta) = \eta^t$ for some integer t coprime to p. Then for $0 \leq i \leq n$ we have:

$$\begin{array}{rrcccl} & \theta\left(\sigma^{p^i} *_r \eta\right) & = & \theta\left(\eta^{d^{rp^i}}\right) & = & \eta^{td^{rp^i}} \\ \text{and} & \sigma^{p^i} *_s \theta(\eta) & = & \sigma^{p^i} *_s \eta^t & = & \eta^{td^{sp^i}}, \end{array}$$

so θ is G_i-equivariant if and only if $d^{rp^i} \equiv d^{sp^i} \pmod{p^n}$. Since d has order p^{n-1} in $(\mathbb{Z}/p^n\mathbb{Z})^\times$, this occurs if and only if $rp^i \equiv sp^i \pmod{p^{n-1}}$, that is, if and only if $r \equiv s \pmod{p^{n-1-i}}$. □

Corollary 4.3. *Let $0 \leq i \leq n-1$. Then:*

1. *The collection $\{K_i \otimes_K H_1, \ldots, K_i \otimes_K H_{p^{n-1}}\}$ can be partitioned into p^{n-1-i} Hopf algebra isomorphism classes;*
2. *Each class contains p^i Hopf algebras;*
3. *$\{K_i \otimes H_1, \ldots, K_i \otimes_K H_{p^{n-1-i}}\}$ is a complete set of representatives for the classes;*

4. *For $0 < j \leq p^{n-1}$, the class containing $K_i \otimes_K H_j$ is*

$$\{K_i \otimes_K H_{j+p^{n-i}m} \mid 0 \leq m < p^i\}.$$

Corollary 4.4. *Let $0 < r \leq p^{n-1}$ and $0 \leq i \leq n-1$. Then $K_i \otimes_K H_r \cong K_i[N]$ as K_i-Hopf algebras if and only if $r \equiv 0 \pmod{n-1-i}$*

We now impose the additional assumptions that K has characteristic zero and contains a primitive p^n-th root of unity ζ; in this case we can use Corollary 3.6 to determine which of the K-Hopf algebras appearing in the classification of Hopf-Galois structures on L/K are isomorphic as K-algebras.

Theorem 4.5. *For $0 < r, s \leq p^{n-1}$, we have $H_r \cong H_s$ as K-algebras if and only if $v_p(r) = v_p(s)$, where v_p denotes the p-adic valuation function.*

Proof. By Corollary 3.6, we have $H_r \cong H_s$ if and only if $(N, *_r) \cong (N, *_s)$ as G-sets, so we must show that this occurs if and only if $v_p(r) = v_p(s)$.

Suppose first that $v_p(r) = v_p(s)$. Then since $\mathrm{Aut}(N)$ is cyclic we must have $\langle \delta^r \rangle = \langle \delta^s \rangle$, and we have $\overline{\beta_r}(G) = \overline{\beta_s}(G)$. Therefore for each $\mu \in N$, the orbits of μ with respect to $*_r$ and $*_s$ coincide, and so the stabilizers $\mathrm{Stab}_r(\mu), \mathrm{Stab}_s(\mu)$ of μ with respect to $*_r, *_s$ have the same order. Since G is cyclic, this implies that they are equal.

Now let $\eta_1, \ldots, \eta_k$ be representatives for the orbits of $(N, *_r)$, and define $\pi : N \to N$ by setting $\pi(\eta_i) = \eta_i$ for each i, and insisting that $\pi(g *_r \mu) = g *_s \pi(\mu)$ for all $\mu \in N$. It is routine to verify that π is well defined and injective, and so it is a G-equivariant bijection from $(N, *_r)$ to $(N, *_s)$.

Conversely, suppose that $v_p(r) \neq v_p(s)$, and assume without loss of generality that $v_p(r) < v_p(s)$. Then since $\mathrm{Aut}(N)$ is cyclic we have $\overline{\beta_s}(G) \subsetneq \overline{\beta_r}(G)$, and so (for example) the orbit of η with respect to $*_s$ is strictly contained in the orbit of η with respect to $*_r$. Therefore $(N, *_r)$ and $(N, *_s)$ cannot be isomorphic G-sets in this case. □

Corollary 4.6. *Precisely n non-isomorphic K-algebras appear in the classification of Hopf-Galois structures on L/K. For each $0 \leq v \leq n-1$, the K-algebra H_{p^v} has $\varphi(p^{n-1-v})$ distinct Hopf-Galois actions on L/K.*

We now explicitly compute the Wedderburn-Artin decompositions of these algebras. Using a result of Bley and Boltje [1, Lemma 2.5], for $0 < r \leq p^{n-1}$ we have

$$H_r = L[\alpha_r(N)]^G \cong \prod_{m=1}^{t} L^{S_m} \text{ as } K\text{-algebras},$$

where the S_m are the stabilizers of a set of representatives of the orbits of G in $\widehat{\alpha_r(N)}$. By Corollary 3.6, these stabilizers coincide with those of a set of representatives of the orbits of G in N, with G acting by

$$\sigma^i *_r \eta^j = \overline{\beta_r}(\sigma^i)[\eta^j] = \delta^{ir}[\eta^j] = \eta^{jd^{ir}}.$$

Since N is cyclic, we may translate this to an action of the additive group $\mathbb{Z}/p^n\mathbb{Z}$ on itself via

$$i \cdot_r j = jd^{ir},$$

and study the orbits and stabilizers of this action.

Lemma 4.7. *Let $j \in \mathbb{Z}/p^n\mathbb{Z}$ and $m = \max\{n - 1 - v_p(j) - v_p(r), 0\}$. Then*

$$\mathcal{O}(j) = \{jd^{ir} : 0 \leq i < p^m\}, \textit{ and Stab}(j) = \langle p^m \rangle.$$

Proof. Note $i \cdot_r j = j$ if and only if

$$jd^{ir} \equiv j \pmod{p^n}$$

i.e.,

$$d^{ir} \equiv 1 \pmod{p^{n-v_p(j)}},$$

which holds if and only if

$$ir \equiv 0 \pmod{p^{n-v_p(j)-1}}.$$

Now if $m = 0$ then $v_p(r) = n - 1 - v_p(j)$, hence $p^{n-1-v_p(j)} \mid r$ and the result is clear. Otherwise, the above congruence holds if and only if

$$i \equiv 0 \pmod{p^{n-1-v_p(j)-v_p(r)}}.$$

Thus, $\text{Stab}(j) = \langle p^{n-1-v_p(j)-v_p(r)} \rangle$. The orbit computation follows immediately. □

The following allows us to count orbit classes in the cases $m > 0$.

Lemma 4.8. *Pick, if possible,* $0 < m \leq n - 1 - v_p(r)$. *Then* $\mathbb{Z}/p^n\mathbb{Z}$ *has* $p^{v_p(r)}(p-1)$ *distinct orbits whose stabilizer is* $\langle p^m \rangle$.

Proof. There are $\varphi(p^{m+v_p(r)+1}) = p^{m+v_p(r)}(p-1)$ elements of order $p^{m+v_p(r)+1}$ in $\mathbb{Z}/p^n\mathbb{Z}$. Clearly, j has order $p^{m+v_p(r)+1}$ if and only if $v_p(j) = n - m - v_p(r) - 1$. Thus, there are $p^{m+v_p(r)}(p-1)$ choices of j for which $m = n - 1 - v_p(j) - v_p(r)$. By Lemma 4.7 there are p^m choices for j in each orbit. Thus, the number of orbits whose stabilizer is $\langle p^m \rangle$ is

$$\frac{p^{m+v_p(r)}(p-1)}{p^m} = p^{v_p(r)}(p-1).$$

□

For $m = 0$ we have

Lemma 4.9. *Suppose* $v_p(j) \geq n - 1 - v_p(r)$. *Then*

$$\mathcal{O}(j) = \{j\} \text{ and } Stab(j) = \mathbb{Z}/p^n\mathbb{Z}.$$

Proof. Immediate from Lemma 4.7 since $m = 0$. Note additionally that there are $p^{1+v_p(r)}$ such j since

$$\{j : v_p(j) \geq n - 1 - v_p(r)\} = \{j' p^{n-1-v_p(r)} : 0 \leq j' < p^{1+v_p(r)}\}.$$

□

Having computed orbits and stabilizers, we are now able to give Wedderburn-Artin decompositions.

Theorem 4.10. *There is an isomorphism of* K*-algebras*

$$H_r \cong K^{p^{1+v_p(r)}} \times \prod_{m=1}^{n-1-v_p(r)} (K_m)^{p^{v_p(r)}(p-1)}.$$

Finally, we use the results of this section to justify our earlier remark that parts (3) and (5) of Corollary 3.6 are not equivalent if the ground field does not contain an appropriate root of unity. We require the following general lemma.

Lemma 4.11. *Let p be an odd prime number, $C = \langle c \rangle$ a cyclic group of order p^n, and A a group with two different actions $*_1, *_2$ on C via automorphisms. Let d be a primitive root modulo p^n, and suppose that there exists $\pi \in A$ such that $\pi *_i c = c^d$ for $i = 1, 2$. Then $(C, *_1) \cong (C, *_2)$ as A-groups if and only if $(C, *_1) \cong (C, *_2)$ as A-sets.*

Proof. Obviously if $(C, *_1) \cong (C, *_2)$ as A-groups then $(C, *_1) \cong (C, *_2)$ as A-sets; we must prove the converse. Suppose that $f : C \to C$ is an A-equivariant bijection. Then in particular $f(\pi *_1 c) = \pi *_2 f(c)$, so $f(c^d) = f(c)^d$, and so $f(c^{d^r}) = f(c)^{d^r}$ for all $r \in \mathbb{Z}$. Since d is a primitive root modulo p^n, this implies that $f(c^k) = f(c)^k$ for all k coprime to p^n. Since f is a bijection, it also implies that the order of $f(c)$ is at least $\varphi(p^n) = p^{n-1}(p-1)$, and therefore exactly p^n. Therefore the homomorphism $g : C \to C$ defined by $g(c) = f(c)$ is an isomorphism. We claim that it is A-equivariant. It is sufficient to show that $g(\alpha *_1 c) = \alpha *_2 g(c)$ for all $\alpha \in A$. Since C is cyclic, there exists $e \in \mathbb{Z}$, coprime to p^n, such that $\alpha *_1 c = c^e$. Now we have:

$$\begin{aligned}
\alpha *_2 g(c) &= \alpha *_2 f(c) \\
&= f(\alpha *_1 c) \\
&= f(c^e) \\
&= f(c)^e \text{ (since } e \text{ is coprime to } p^n) \\
&= g(c)^e \\
&= g(c^e) \text{ (} g \text{ is a homomorphism)} \\
&= g(\alpha *_1 c).
\end{aligned}$$

Thus g is A-equivariant, and so $(C, *_1) \cong (C, *_2)$ as A-groups. □

Now we construct an example of a cyclic extension L/K for which K does not contain a primitive $|N|^{\text{th}}$ root of unity, $(N, *_1) \cong (N, *_2)$ as Γ-sets, but $(\widehat{N}, *_1) \ncong (\widehat{N}, *_2)$ as Γ-sets. We remark that this implies that the corresponding Hopf algebras are isomorphic as coalgebras, but not as algebras.

Example 4.12. Let $L = \mathbb{Q}(\zeta_{19} + \zeta_{19}^{-1})$, the maximal real subfield of $\mathbb{Q}(\zeta_{19})$. Then $L/\mathbb{Q}$ is cyclic of degree 9; write $G = \langle \sigma \rangle$ for its Galois group and let $\Gamma = \mathrm{Gal}(\mathbb{Q}^{\mathrm{sep}}/\mathbb{Q})$. There are precisely three Hopf-Galois structures on $L/\mathbb{Q}$, and they all have cyclic type. Let $N = \langle \eta \rangle$ be an abstract cyclic group of order

9. Then the embeddings of G into $\mathrm{Hol}(N) = \rho(N) \rtimes \mathrm{Aut}(N)$ corresponding to the Hopf-Galois structures on L/K are

$$\beta_s(\sigma) = (\rho(\eta), \delta^s), 0 \leq s < 3,$$

where $\delta(\eta) = \eta^4$. Each of these embeddings yields an action of G on N by automorphisms: $\sigma *_s \eta = \delta^s(\eta)$. In particular, we have $\sigma *_1 \eta = \eta^4$ and $\sigma *_2 \eta = \eta^7$. It is easily verified that the bijection $N \to N$ defined by

$$\begin{array}{lll} f(1) = 1 & f(\eta) = \eta & f(\eta^2) = \eta^2 \\ f(\eta^3) = \eta^3 & f(\eta^4) = \eta^7 & f(\eta^5) = \eta^8 \\ f(\eta^6) = \eta^6 & f(\eta^7) = \eta^4 & f(\eta^8) = \eta^5 \end{array}$$

is G-equivariant, so $(N, *_1) \cong (N, *_2)$ as G-sets, and hence as Γ-sets, since the action of Γ on N factors through G. Note, however, that there is no Γ-equivariant automorphism of N, since by Theorem 4.2 the Hopf algebras giving the Hopf-Galois structures corresponding to β_1, β_2 are not isomorphic as Hopf algebras.

Now we consider $\widehat{N}$. Let $\chi : N \to \mathbb{Q}^{\mathrm{sep}}$ be defined by $\chi(\eta) = \zeta_9$; then $\widehat{N} = \langle \chi \rangle$. The two actions of Γ on $\widehat{N}$ (corresponding to the actions $*_1, *_2$ of Γ on N) both factor through $\mathrm{Gal}(L\mathbb{Q}(\zeta_9)/\mathbb{Q})$, which is isomorphic to $G \times \mathrm{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q})$ since L and $\mathbb{Q}(\zeta_9)$ are linearly disjoint over $\mathbb{Q}$. Let π be the generator of $\mathrm{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q})$ defined by $\pi(\zeta_9) = \zeta_9^2$. It is easy to verify that $\pi *_i \chi = \chi^2$ for each i, and so $\widehat{N}$ satisfies the hypotheses of Lemma 4.11. Therefore, if we had $(\widehat{N}, *_1) \cong (\widehat{N}, *_2)$ as Γ-sets then we would have $(\widehat{N}, *_1) \cong (\widehat{N}, *_2)$ as Γ-groups, and so $(N, *_1) \cong (N, *_2)$ as Γ-groups. But we noted above that this is impossible. Therefore we have $(N, *_1) \cong (N, *_2)$ as Γ-sets, but $(\widehat{N}, *_1) \ncong (\widehat{N}, *_2)$ as Γ-sets.

[1] Bley, W., Boltje, R., 1999. Lubin-Tate formal groups and module structure over Hopf orders. Journal de théorie des nombres de Bordeaux 11, 269–305.

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

[3] Byott, N. P., 2002. Integral Hopf Galois structures on degree p^2 extensions of p-adic fields. Journal of Algebra 248, 334–365.

[4] Byott, N. P., 2004. Hopf Galois structures on Galois field extensions of degree pq. J. Pure Appl. Algebra 188 (1-3), 45–57.

[5] Childs, L. N., 2000. Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory. Vol. 80. American Mathematical Society, Mathematical Surveys and Monographs.

[6] Childs, L. N., 2011. Hopf Galois structures on Kummer extensions of prime power degree. New York J. Math 17, 51–74.

[7] Childs, L. N., 2013. Fixed-point free endomorphisms and Hopf Galois structures. Proceedings of the American Mathematical Society 141(4), 1255–65.

[8] Childs, L. N., Corradino, J., 2007. Cayley's theorem and Hopf Galois structures on for semidirect products of cyclic groups. Journal of Algebra 308, 236–251.

[9] Crespo, T., Rio, A., Vela, M., 2015. Non-isomorphic Hopf-Galois structures with isomorphic underlying Hopf algebras. Journal of Algebra 422, 270–276.

[10] Greither, C., Pareigis, B., 1987. Hopf Galois theory for separable field extensions. Journal of Algebra 106, 239–258.

[11] Koch, A., 2014. Hopf Galois structures on primitive purely inseparable extensions. New York Journal of Mathematics 20, 779–797.

[12] Koch, A., Kohl, T., Truman, P. J., Underwood, R., to appear. The structure of Hopf algebras acting on dihedral extensions. In: C. Pillen, e. a. (Ed.), Advances in Algebra: Research from the Southern Regional Algebra Conference 2017. Proc. in Math. Stat. Springer.

[13] Kohl, T., 1998. Classification of the Hopf Galois structures on prime power radical extensions. Journal of Algebra 207, 525–546.

[14] Truman, P. J., 2016. Hopf Galois module structure of tame $C_p \times C_p$ extensions. Journal de théorie des nombres de Bordeaux 28.2, 557–582.

[15] Waterhouse, W. C., 1979. Introduction to affine group schemes. No. 66 in GTM. Springer, New York.