New York Journal of Mathematics

New York J. Math. **23** (2017) 1–10.

On the Galois correspondence for Hopf Galois structures

Lindsay N. Childs

Abstract. We study the question of the surjectivity of the Galois correspondence from subHopf algebras to subfields given by the Fundamental Theorem of Galois Theory for abelian Hopf Galois structures on a Galois extension of fields with Galois group Γ, a finite abelian p-group. Applying the connection between regular subgroups of the holomorph of a finite abelian p-group $(G, +)$ and associative, commutative nilpotent algebra structures A on $(G, +)$, we show that if A gives rise to a H-Hopf Galois structure on L/K, then the K-subHopf algebras of H correspond to the ideals of A. Among the applications, we show that if G and Γ are both elementary abelian p-groups, then the only Hopf Galois structure on L/K of type G for which the Galois correspondence is surjective is the classical Galois structure.

Contents

1. Introduction

The Fundamental Theorem of Galois Theory (FTGT) of Chase–Sweedler [ChaS69] states that if L/K is a H-Hopf Galois extension of fields for H a K-Hopf algebra, then there is an injection $\mathcal{F}$ from the set of K-sub-Hopf algebras of H to the set of intermediate fields $K \subseteq E \subseteq L$ given by sending a K-subHopf algebra J to $\mathcal{F}(J) = L^J$. The *strong form* of the FTGT holds if the injection is also a surjection. For a classical Galois extension of fields

Received December 5, 2016.
2010 *Mathematics Subject Classification.* Primary 12F10, secondary 13M05.
Key words and phrases. Hopf Galois extension, finite commutative nilpotent ring, Fundamental Theorem of Galois Theory.

ISSN 1076-9803/2017

with Galois group Γ, the FTGT holds in its strong form. It is known from [GP87] that if L/K is a (classical) Galois extension with nonabelian Galois group Γ, then there is a Hopf Galois structure on L/K so that $\mathcal{F}$ maps onto the subfields E of L that are normal over K. So if Γ is not a Hamiltonian group [Ha59, 12.5], then L/K has a Hopf Galois structure for which the strong form of the FTGT does not hold. In particular, the strong form fails extremely for the unique [By04] nonclassical Hopf Galois structure on L/K when Γ is a nonabelian simple group.

Nearly all of the examples examining the success or failure of the strong form of the FTGT for a nonclassical Hopf Galois structure on a classical Galois extension L/K with Galois group Γ involve nonabelian groups. Perhaps the only wholly abelian example of failure in the literature is in [CrRV15], 2.2, where $\Gamma \cong C_2 \times C_2$ and L/K has a Hopf Galois structure by H, a K-Hopf algebra which is a K-form of LC_4. Then by classical Galois theory, there are three intermediate subfields between K and L, but LC_4 has only one intermediate L-Hopf algebra, so H can have at most one intermediate K-subHopf algebra. Hence the strong form of the FTGT cannot hold for that Hopf Galois structure.

Here we assume that L/K is a Galois extension with Galois group an abelian p-group Γ of order p^n. Suppose L/K also has a H-Hopf Galois structure by an abelian (commutative and cocommutative)K-Hopf algebra H. We will characterize the K-sub-Hopf algebras of H. Since we know by the classical FTGT that the intermediate fields between K and L are bijective with the subgroups of Γ, it will be easy to compare the number of subgroups of Γ with the number of K-sub-Hopf algebras of G, and thereby better understand how far the Galois correspondence for H is from being surjective.

The new tool in our study is the correspondence between regular subgroups of the holomorph of a finite abelian p-group $G = (G, +)$ and associative, commutative nilpotent ring structures $A = (G, +, \cdot)$ on the additive group G. This correspondence was presented for G an elementary abelian p-group by A. Caranti, F. Dalla Volta and M. Sala in [CDVS06] and extended to all finite abelian p-groups in [FCC12].

This paper and [FCC12], [Chi15] and [Chi16] demonstrate in different ways the usefulness of the correspondence of [CDVS06] in the Hopf Galois theory of Galois extensions of fields whose Galois group is a finite abelian p-group.

2. Some translations

Let L/K be a Galois extension with Galois group Γ and let G be a group of the same cardinality as Γ. Let H be a K-Hopf algebra and $H \otimes_K L \to L$ be an H-module algebra action that makes L/K into an H-Hopf Galois extension. We will need three successive translations of the data: the K-Hopf algebra H, and the action of H on L.

The first translation. This is the main result of Greither and Pareigis [GP87]. By "base change" from K to L, the K-Hopf algebra H and its action on L becomes the L-Hopf algebra $L \otimes_K H$ and the lifted action of $L \otimes_K H$ on $L \otimes_K L$. Since L/K is a Galois extension with Galois group Γ,

$$L \otimes_K L \cong \Gamma L = \oplus_{\gamma \in \Gamma} L e_\gamma$$

where $\{e_\gamma : \gamma \in \Gamma\}$ is a dual basis to the elements γ of Γ, and as Greither and Pareigis point out, it follows that $L \otimes_K H$ is a group ring LN where LN acts on ΓL as a regular group of permutations of the dual basis of Γ, and $N \subset \mathrm{Perm}(\Gamma)$ is normalized by the image $\lambda(\Gamma)$ of the left regular representation of Γ in $\mathrm{Perm}(\Gamma)$. This base change is bijective, because given a regular subgroup N of $\mathrm{Perm}(\Gamma)$ normalized by $\lambda(\Gamma)$ and an action of LN on ΓL, the regularity of N implies that the action of LN on ΓL makes the extension $\Gamma L/L$ into an LN-Hopf Galois extension. Since N is normalized by $\lambda(\Gamma)$, Galois descent of the Hopf Galois extension over L (that is, taking fixed subrings under the action of Γ acting on L by the action of the Galois group of L/K and on N by conjugation by $\lambda(\Gamma)$) yields H and the original Hopf Galois structure of H on L over K.

Of relevance for us concerning this translation is a result of Crespo, Rio and Vela ([CrRV16], Proposition 2.2), that in the setting of the last paragraph, the K-subHopf algebras of H correspond to the subgroups of N that are normalized by $\lambda(\Gamma)$.

The second translation. Let N be a regular subgroup of $\mathrm{Perm}(\Gamma)$ normalized by $\lambda(\Gamma)$. Then N has the same order as $\lambda(\Gamma)$. Let G be an abstract group of the same cardinality of Γ such that there is an isomorphism $\alpha : G \to N$. Then we say that the corresponding K-Hopf algebra H has *type* G. Viewing N as a subgroup of $\mathrm{Perm}(\Gamma)$, the map $\alpha : G \to \mathrm{Perm}(\Gamma)$ is a regular embedding of G in $\mathrm{Perm}(\Gamma)$.

As shown in [By96], a regular embedding $\alpha : G \to \mathrm{Perm}(\Gamma)$ whose image $\alpha(G)$ is normalized by $\lambda(\Gamma)$ corresponds to a regular embedding

$$\beta : \Gamma \to \mathrm{Hol}(G),$$

where

$$\mathrm{Hol}(G) = \rho(G)\mathrm{Aut}(G) \subset \mathrm{Perm}(G)$$

is the normalizer of $\lambda(G)$ in $\mathrm{Perm}(G)$. Here $\rho : G \to \mathrm{Perm}(G)$ is the right regular representation of G in $\mathrm{Perm}(G)$. The relationship between α and β is as follows:

Let $\beta : \Gamma \to \mathrm{Hol}(G)$ be a regular embedding. Define $b : \Gamma \to G$ by

$$b(\gamma) = \beta(\gamma)(e_G)$$

for γ in Γ, where e_G is the identity element of G. Then for all g in G,

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

Define $\alpha : G \to \mathrm{Perm}(\Gamma)$ by

$$\alpha(g)(\gamma) = (b^{-1}(\lambda(g))b)(\gamma) = (C(b^{-1})\lambda(g))(\gamma).$$

Then $\alpha(g)(e_\Gamma) = b^{-1}(g)$ and $C(b)\lambda(\gamma) = \beta$. Then $\alpha(G)$ is normalized by $\lambda(\Gamma)$. In fact,

Proposition 2.1. *Suppose $\beta : \Gamma \to \mathrm{Hol}(\lambda(G))$ is a regular embedding, and let $\alpha = C(b^{-1})\lambda : G \to \mathrm{Perm}(\Gamma)$ be the regular embedding corresponding to β. Then for all γ in Γ and g in G, there is some h in G so that*

$$\beta(\gamma)\lambda(g)\beta(\gamma)^{-1} = \lambda(h)$$

and

$$\lambda(\gamma)\alpha(g)\lambda(\gamma)^{-1} = \alpha(h).$$

Proof. The first formula follows because β maps Γ into $\mathrm{Hol}(G)$, the normalizer of $\lambda(G)$ in $\mathrm{Perm}(G)$. Since $C(b^{-1})(\beta)(\gamma) = \lambda(\gamma)$ and $C(b^{-1})\lambda(g) = \alpha(g)$, the second formula follows from the first by applying $C(b^{-1})$ to the first formula. □

The third translation. Here is the result of Caranti, et. al. from [FCC12].

Proposition 2.2. *Let $(G, +)$ be a finite abelian p-group. Then each regular subgroup of $\mathrm{Hol}(G)$ is isomorphic to the group $(G, \circ)$ induced from a structure $(G, +, \cdot)$ of a commutative, associative nilpotent ring (hereafter, "nilpotent") on $(G, +)$, where the operation $\circ$ is defined by $g \circ h = g + h + g \cdot h$.*

The idea is the following: Let $(G, +)$ be an abelian group of order p^n , and suppose that $A = (G, +, \cdot)$ is a nilpotent ring structure on $(G, +)$ yielding the operation $\circ$. Define $\tau : (G, \circ) \to \mathrm{Hol}(G, +)$ by $\tau(g)(x) = g \circ x$. Then $\tau(g)(0) = g$, and

$$\tau(g)\tau(g')(x) = \tau(g)(g' \circ x) = g \circ (g' \circ x) = (g \circ g') \circ x = \tau(g \circ g')(x).$$

Thus τ is an isomorphism from $(G, \circ)$ into $\mathrm{Perm}(G, +)$. Since

$$\tau(g)\lambda(g')\tau(g)^{-1} = \lambda(g' + gg'),$$

the image $\tau(G, \circ) = T$ is a regular subgroup of $\mathrm{Hol}(G)$. This process is reversible: given a regular subgroup T of $\mathrm{Hol}(G, +)$, there is a nilpotent ring structure $A = (G, +, \cdot)$ on G, which defines the $\circ$ operation as above and yields a unique isomorphism $\tau : (G, \circ) \to T$ so that $\tau(g)(x) = g \circ x$.

3. Sub-Hopf algebras of H

Suppose L/K be a Galois extension with Galois group Γ, a finite abelian p-group of order p^n. Suppose there is a Hopf Galois structure on L/K by H so that $L \otimes_K H = LN$.

Let $\alpha : G \to N$ be an isomorphism and let $\beta : \Gamma \to T \subset \mathrm{Hol}(G)$ be the regular embedding of Γ in $\mathrm{Hol}(G)$ corresponding to α. Let $A = (G, +, \cdot)$ be the nilpotent ring structure on $(G, +)$ corresponding to T. Let $(G, \circ)$ be the set G with the operation $\circ$ from A, let $\tau : A = (G, \circ) \to T \subset \mathrm{Hol}(G)$ so that $\tau(g)(x) = g \circ x$, and let $\xi : \Gamma \to (G, \circ)$ be an isomorphism so that $\beta = \tau\xi$.

Theorem 3.1. *Suppose the nilpotent algebra $A = (G, +, \cdot)$ yields the regular embedding $\alpha : (G, +) \to \mathrm{Perm}(\Gamma)$ whose image is normalized by $\lambda(\Gamma)$. Let L/K be a Galois extension of fields with Galois group Γ which is a H-Hopf Galois extension where H corresponds to $\alpha(G, +)$. Then the lattice (under inclusion) of $\lambda(\Gamma)$-invariant subgroups of $\alpha(G)$, and hence the lattice of K-sub-Hopf algebras of H, is isomorphic to the lattice of ideals of A.*

Proof. First, $\alpha : G \to \mathrm{Perm}(\Gamma)$ is an injective homomorphism from $(G, +)$ to $\mathrm{Perm}(\Gamma)$. Since α is injective, there is a bijection between subgroups of $(G, +)$ and subgroups of $\alpha(G)$. Clearly $J_1 \subseteq J_2$ iff $\alpha(J_1) \subseteq \alpha(J_2)$, so the bijection is lattice-preserving.

Suppose the image $\alpha(G)$ of α is normalized by $\lambda(\Gamma)$, so for all γ in Γ, g in G, there is some h in G so that

$$\lambda(\gamma)\alpha(g)\lambda(\gamma)^{-1} = \alpha(h).$$

By Proposition 2.1, this equation holds iff

$$\beta(\gamma)\lambda(g) = \lambda(h)\beta(\gamma).$$

Recalling that $A = (G, +, \cdot) = (G, \circ)$, factor $\beta = \tau\xi$ where

$$\xi : \Gamma \to A = (G, \circ)$$

is an isomorphism and $\tau : A = (G, \circ) \to \mathrm{Hol}(G)$ sends k in G to $\tau(k)$ where $\tau(k)(y) = k \circ y$ for y in G. Let $\xi(\gamma) = k$ in A. Then the last equation is

$$\tau(k)\lambda(g) = \lambda(h)\tau(k),$$

and applying this to x in G gives

$$\tau(k)(g + x) = h + \tau(k)(x).$$

Since $\tau(k)(x) = k \circ x$, we have

$$k \circ (g + x) = h + k \circ x.$$

Viewing this equation in A, where $a \circ b = a + b + a \cdot b$, we have

$$k + (g + x) + k \cdot g + k \cdot x = h + k + x + k \cdot x.$$

This last equation reduces to

$$h = g + k \cdot g.$$

Now suppose J is an ideal of A and g is in J. Then $k \cdot g$ is in J, so h is in J, and so $\lambda(\gamma)$ conjugates $\alpha(g)$ in $\alpha(J)$ to an element of $\alpha(J)$. So $\alpha(J)$ is normalized by $\lambda(\Gamma)$ in $\mathrm{Perm}(\Gamma)$.

Conversely, suppose J is an additive subgroup of $(G, +, \cdot) = A$ and $\alpha(J)$ is normalized by $\lambda(\Gamma)$. Then for all γ in G, g in J,

$$\lambda(\gamma)\alpha(g)\lambda(\gamma)^{-1} = \alpha(h)$$

and $\alpha(h)$ is in $\alpha(J)$. So h is in J. Then by Proposition 2.1 as above, for all $k = \xi(\gamma)$ in G, and g in J, $h = g + k \cdot g$ is in J. Now J is an additive subgroup of A, so $k \cdot g$ is in J for all k in G, g in J. Thus J is an ideal of A. □

4. Examples

Theorem 3.1 transforms the problem of describing the image of the Galois correspondence map $\mathcal{F}$ on a H-Hopf Galois structure on L/K to the study of the ideals of the nilpotent algebra associated to H. In this section we look at some examples.

Theorem 4.1. *Let L/K be a Galois extension of fields with Galois group Γ an elementary abelian p-group of order p^n. Let L/K have a Hopf Galois structure by an abelian Hopf algebra H of type G where G is an elementary abelian p-group. Let A be the nilpotent ring structure yielding the regular subgroup $T \cong (G, \circ) \subset \mathrm{Hol}(G)$ corresponding to H, where $(G, \circ) \cong \Gamma$. Then the H-Hopf Galois structure on L/K satisfies the strong form of the FTGT if and only if H is the classical Galois structure by $K\Gamma$ on L/K.*

Proof. If $A^2 = 0$, then $(G, \circ) = (G, +)$, so the regular subgroup T acts on G by $\tau(g)(h) = g \circ h = g + h$, hence $T = \lambda(G)$. Since G is abelian, the corresponding Hopf Galois structure on L/K is the classical structure by the K-Hopf algebra $K[\Gamma]$. So the Galois correspondence holds in its strong form.

For the converse, view $(G, +)$ as an n-dimensional $\mathbb{F}_p$-vector space. Suppose $A^2 \neq 0$. Then for some a, b in A, $ab \neq 0$. Then the subspace $\mathbb{F}_p a$ does not contain ab. For if $ab = ra$ for $r \neq 0$ in $\mathbb{F}_p$, then $a = sba$ for $s \neq 0$ in $\mathbb{F}_p$. Then

$$a = (sb)a = (sb)^2 a = \ldots = (sb)^{n+1} a = 0$$

since A is nilpotent of dimension n, hence $(sb)^{n+1} = 0$. Thus the subspace $\mathbb{F}_p a$ is not an ideal of A.

The subgroup $\alpha(\mathbb{F}_p a)$ of $\alpha(G)$ is then not normalized by $\lambda(\Gamma)$. But $\Gamma \cong G$, so there are bijections between subgroups of $\alpha(G)$, subgroups of G, subgroups of Γ and (by classical Galois theory) subfields of L containing K. If some subgroup of $\alpha(G)$ is not normalized by $\lambda(\Gamma)$, then the number of K-subHopf algebras of $H = L[\alpha(G)]^G$ is strictly smaller than the number of subfields between K and L. So the Galois correspondence for the H-Hopf Galois structure on L/K does not hold in its strong form. □

There are many examples. If G is an elementary abelian p-group of order p^n with p odd, and $T \cong (G, \circ)$ is a regular subgroup of $\mathrm{Hol}(G)$ corresponding to a nilpotent ring structure $A = (G, +, \cdot)$ with $A^p = 0$, then $(G, \circ)$ is an abelian group of exponent p by Caranti's Lemma ([Chi15], Proposition 2.2), so is isomorphic to G. Hence every isomorphism type of nilpotent $\mathbb{F}_p$-algebra A of dimension n with $A^p = 0$ yields a Hopf Galois structure on a Galois extension L/K with Galois group $\Gamma \cong G$. As n goes to infinity, the number of such Hopf Galois structures is asymptotic to $p^{\frac{2}{27}n^3}$ ([Chi15], Theorem 10.3).

By choosing a particular nilpotent algebra structure on $(\mathbb{F}_p^n, +)$ we can see how badly the Galois correspondence can fail to be surjective.

Let A be the primitive n-dimensional nilpotent $\mathbb{F}_p$-algebra generated by z with $z^{n+1} = 0$. Then $(A, +) \cong (\mathbb{F}_p^n, +)$ and so the multiplication on A yields a nilpotent $\mathbb{F}_p$-algebra structure on $(G, +) = (\mathbb{F}_p^n, +)$. Let $G = (\mathbb{F}_p^n, \circ)$ where the operation $\circ$ is defined using the multiplication on A by $a \circ b = a + b + a \cdot b$.

Theorem 4.2. *Let G be an elementary abelian p-group of order p^n. Let A be a primitive $\mathbb{F}_p$-algebra structure A on G, and let $(G, \circ)$ be the corresponding group structure on $\mathbb{F}_p^n$. Suppose L/K is a Galois extension of fields with Galois group $\Gamma \cong (G, \circ)$. Then the primitive nilpotent $\mathbb{F}_p$-algebra A corresponds to an H-Hopf Galois structure on L/K for some K-Hopf algebra H, and the K-subHopf algebras of H form a descending chain*

$$H = H_1 \supset H_2 \supset \ldots \supset H_n \supset K.$$

Hence the Galois correspondence $\mathcal{F}$ for H maps onto exactly $n+1$ fields F with $K \subseteq F \subseteq L$.

Proof. Given Theorem 3.1, we just need to show that ideals of A are $J_i = \langle z^i \rangle$ for $i = 1, \ldots, n$.

Suppose J is a nonzero ideal of A and contains $s(z^k + z^{k+r}b)$ of minimal degree k, where $s \neq 0$ in $\mathbb{F}_p$, b in A and $r \geq 1$. Then J also contains

$$z^k + z^{k+r}b$$

and

$$(z^k + z^{k+r}b)(-z^r b) = -z^{k+r}b - z^{k+2r}b^2,$$

hence their sum,

$$z^k - z^{k+2r}b^2 = z^k + z^{k+r'}b'$$

for some b' in A, where $r' > r$. Repeating this argument until $r' > n$ shows that J contains z^k, hence $J \supseteq J_k = \langle z^k \rangle$. Since $J_k = \langle z^k \rangle$ contains every element of degree $\geq k$, $J = J_k$. Thus A has exactly $n+1$ ideals. Since the correspondence between ideals of A and $\lambda(\Gamma)$ invariant subgroups of $\alpha(G)$ is lattice-preserving, we have a single filtration

$$\alpha(G) = \alpha(J_1) \supset \alpha(J_2) \supset \ldots \supset \alpha(J_n) \supset 0.$$

of $\lambda(G)$-invariant subgroups of $\alpha(G)$. If H is the corresponding K-Hopf algebra making L/K into a Hopf Galois extension, then H has a unique filtration of K-sub-Hopf algebras,

$$H = H_1 \supset H_2 \supset \ldots \supset H_n \supset K.$$ □

For A a primitive nilpotent $\mathbb{F}_p$-algebra with $A^{n+1} = 0$, the corresponding group $(G, \circ)$ is isomorphic (by $a \mapsto 1 + a$) to the group of principal units of the truncated polynomial ring $\mathbb{F}_p[x]/(x^{n+1}\mathbb{F}_p[x])$. The structure of that group is described in Corollary 3 of [Chi07]. In particular $(G, \circ)$, hence Γ, is an elementary abelian p-group if and only if $p > n$.

Thus in Theorem 4.2, when $p > n$, then L/K is classically Galois with Galois group $\Gamma \cong (\mathbb{F}_p^n, +)$. So the number of subgroups of Γ, and hence the number of subfields E with $K \subseteq E \subseteq L$, is equal to the number of subspaces of $\mathbb{F}_p^n$, namely

$$\sum_{r=1}^{n} \frac{(p^n-1)(p^n-p)\cdots(p^n-p^{r-1})}{(p^r-1)(p^r-p)\cdots(p^r-p^{r-1})} \geq p^{\lfloor \frac{n^2}{4} \rfloor}.$$

So the Galois correspondence map $\mathcal{F}$ is extremely far from being surjective for a Hopf Galois structure corresponding to a nilpotent algebra structure A with $\dim(A/A^2) = 1$.

By contrast:

Proposition 4.3. *Let L/K be a Galois extension of fields with Galois group Γ cyclic of order p^n, p odd. Let the K-Hopf algebra H give a Hopf Galois structure on L/K. Then H has type G where $G \cong \Gamma$, and the Galois correspondence for that Hopf Galois structure holds in its strong form.*

Proof. From [Ko98] it is known that if Γ is cyclic of order p^n then every Hopf Galois structure must have type $G \cong \Gamma$. So let G be cyclic of order p^n, which we identify with $(\mathbb{Z}/p^n\mathbb{Z}, +)$. Then we view $\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G)$ as the set of pairs (a, g) where a and g are modulo p^n and $(g, p) = 1$, or equivalently as the set of matrices

$$\begin{pmatrix} g & a \\ 0 & 1 \end{pmatrix}$$

in $\mathrm{Aff}_1(\mathbb{Z}/p^n\mathbb{Z}) \subset \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$, acting on s in G by

$$\begin{pmatrix} g & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} s \\ 1 \end{pmatrix} = \begin{pmatrix} gs + a \\ 1 \end{pmatrix}.$$

View Γ as the free $\mathbb{Z}/p^n\mathbb{Z}$-module with basis y. From Proposition 2 of [Chi11], the p^{n-1} regular embeddings $\beta : \Gamma = (\mathbb{Z}/p^n\mathbb{Z})y \to \mathrm{Hol}(G)$ are determined by $\beta(y)$ where

$$\beta(y) = \begin{pmatrix} 1 + pd & -1 \\ 0 & 1 \end{pmatrix}$$

for some d modulo p^{n-1}. So in the notation above Theorem 3.1, $\xi(y) = -1$ in $G = \mathbb{Z}/p^n\mathbb{Z}$ and

$$\tau(-1) = \begin{pmatrix} 1 + pd & -1 \\ 0 & 1 \end{pmatrix},$$

which acts on s in G as above. That action defines the operation $\circ$ on G by

$$(-1) \circ s = (1 + pd)s - 1 = -1 + s + pds.$$

The multiplication on $(G,+)$ to make $(G,+,\cdot) = A$ a nilpotent algebra is then defined by

$$(-1) \cdot s = (-1) \circ s - ((-1) + s) = (-1 + s + pds) + 1 - s = pds.$$

By distributivity, for every r, s in $\mathbb{Z}/p^n\mathbb{Z}$,

$$-r \cdot s = rspd.$$

Replacing d by $-d$, let A_d be the commutative nilpotent algebra structure on $(\mathbb{Z}/p^n\mathbb{Z},+)$ with multiplication

$$r \cdot s = rspd$$

for all r, s in $\mathbb{Z}/p^n\mathbb{Z}$. It is then easy to check that the ideals of A_d are the principal ideals generated by p^r, for $r = 0, \dots, n$. Since those are also the additive subgroups of $(A_d,+) = (\mathbb{Z}/p^n\mathbb{Z},+)$, it follows by Theorem 3.1 that for every Hopf Galois structure on L/K, the Galois correspondence holds in its strong form. □

Information on finite commutative nilpotent $\mathbb{F}_p$-algebras may be found in [Chi15] and the references listed there, notably [Po08].

My thanks to the referee for a careful reading of the manuscript.

References

[By96] Byott, Nigel P. Uniqueness of Hopf Galois structure of separable field extensions. *Comm. Algebra* **24** (1996), no. 10, 3217–3228. MR1402555, Zbl 0878.12001, doi: 10.1080/00927879608825743.

[By04] Byott, Nigel P. Hopf–Galois structures on field extensions with simple Galois groups. *Bull. London Math. Soc.* **36** (2004), no. 1, 23–29. MR2011974, Zbl 1038.12002, doi: 10.1112/S0024609303002595.

[CDVS06] Caranti, Andrea; Dalla Volta, Francesca; Sala, Massimiliano. Abelian regular subgroups of the affine group and radical rings. *Publ. Math. Debrecen* **69** (2006), no. 3, 297–308. MR2273982, Zbl 1123.20002, arXiv:math/0510166.

[ChaS69] 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, Zbl 0197.01403, doi: 10.1007/BFb0101433.

[Chi89] Childs, Lindsay N. On the Hopf Galois theory for separable field extensions. *Comm. Algebra* **17** (1989), no. 4, 809–825. MR0990979, Zbl 0692.12007, doi: 10.1080/00927878908823760.

[Chi07] Childs, Lindsay N. Some Hopf Galois structures arising from elementary abelian p-groups. *Proc. Amer. Math. Soc.* **135** (2007), no. 11, 3453–3460. MR2336557, Zbl 1128.16022, doi: 10.1090/S0002-9939-07-08888-0.

[Chi11] Childs, Lindsay N. Hopf Galois structures on Kummer extensions of prime power degree. *New York J. Math.* **17** (2011), 51–74. MR2781908, Zbl 1233.12003.

[Chi15] Childs, Lindsay N. On Abelian Hopf Galois structures and finite commutative nilpotent rings. *New York J. Math.* **21** (2015), 205–229. MR3336553, Zbl 1318.13030.

[Chi16] Childs, Lindsay N. Obtaining abelian Hopf Galois structures from finite commutative nilpotent rings. Preprint, 2016. arXiv:1604.05269.

[CrRV15] Crespo, Teresa; Rio, Anna; Vela, Montserrat. From Galois to Hopf Galois: theory and practice. *Trends in number theory*, 29–46, Contemp. Math., 649. *Amer. Math. Soc., Providence, RI*, 2015. MR3415265, Zbl 06607874, arXiv:1403.6300, doi: 10.1090/conm/649/13018.

[CrRV16] Crespo, Teresa; Rio, Anna; Vela, Montserrat. On the Galois correspondence theorem in separable Hopf Galois theory. *Publ. Mat.* **60** (2016), no. 1, 221–234. MR3447739, Zbl 1331.12009, arXiv:1405.0881, doi: 10.5565/PUBLMAT_60116_08.

[FCC12] Featherstonhaugh, Stephen C.; Caranti, Andrea; Childs, Lindsay N. Abelian Hopf Galois structures on prime-power Galois field extensions. *Trans. Amer. Math. Soc.* **364** (2012), no. 7, 3675–3684. MR2901229, Zbl 1287.12002, doi: 10.1090/S0002-9947-2012-05503-6.

[GP87] Greither, Cornelius; Pareigis, Bodo. Hopf Galois theory for separable field extensions. *J. Algebra* **106** (1987), no. 1, 239–258. MR0878476, Zbl 0615.12026, doi: 10.1016/0021-8693(87)90029-9.

[Ha59] Hall, Marshall, Jr. The theory of groups. *The Macmillan Co., New York, N.Y.*, 1959. xiii+434 pp. MR0103215, Zbl 0084.02202.

[Ko98] Kohl, Timothy. Classification of the Hopf Galois structures on prime power radical extensions. *J. Algebra* **207** (1998), no. 2, 525–546. MR1644203, Zbl 0953.12003, doi: 10.1006/jabr.1998.7479.

[Po08] Poonen, Bjorn. The moduli space of commutative algebras of finite rank. *J. Eur. Math. Soc. (JEMS)* **10** (2008), no. 3, 817–836. MR2421162, Zbl 1151.14011, arXiv:math/0608491, doi: 10.4171/JEMS/131.

(Lindsay N. Childs) Department of Mathematics and Statistics, University at Albany, Albany, NY 12222
lchilds@albany.edu

This paper is available via http://nyjm.albany.edu/j/2017/23-1.html.