

## ABELIAN HOPF GALOIS STRUCTURES ON PRIME-POWER GALOIS FIELD EXTENSIONS

S. C. FEATHERSTONHAUGH, A. CARANTI, AND L. N. CHILDS

ABSTRACT. The main theorem of this paper is that if  $(N, +)$  is a finite abelian  $p$ -group of  $p$ -rank  $m$  where  $m + 1 < p$ , then every regular abelian subgroup of the holomorph of  $N$  is isomorphic to  $N$ . The proof utilizes a connection, observed by Caranti, Dalla Volta, and Sala, between regular abelian subgroups of the holomorph of  $N$  and nilpotent ring structures on  $(N, +)$ . Examples are given that limit possible generalizations of the theorem. The primary application of the theorem is to Hopf Galois extensions of fields. Let  $L|K$  be a Galois extension of fields with abelian Galois group  $G$ . If also  $L|K$  is  $H$ -Hopf Galois, where the  $K$ -Hopf algebra  $H$  has associated group  $N$  with  $N$  as above, then  $N$  is isomorphic to  $G$ .

### 1. INTRODUCTION

Let  $L|K$  be a Galois extension of fields with (finite) Galois group  $G$ . Then  $L$  is a  $KG$ -Hopf Galois extension of  $K$ , where  $KG$  is the group ring of  $G$  acting on  $L$  via the action by the Galois group  $G$ . As Greither and Pareigis showed [GP87], there may exist  $K$ -Hopf algebras  $H$  other than the group ring  $KG$  that make  $L$  into a Hopf Galois extension of  $K$ . If so, then under base change, the  $L$ -Hopf algebra  $L \otimes_K H$  is isomorphic to the group ring  $LN$  of a regular subgroup  $N$  of  $\text{Perm}(G)$ , the group of permutations of  $G$ . Conversely, if  $N$  is a regular subgroup of  $\text{Perm}(G)$  normalized by  $\lambda(G)$ , the image of the left regular representation of  $G$  in  $\text{Perm}(G)$ , then the action of  $LN$  on  $\text{Hom}_L(LG, L)$  descends to an action of the  $K$ -Hopf algebra  $H = LN^G$  on  $L$ , making  $L|K$  into an  $H$ -Hopf Galois extension. Thus determining Hopf Galois structures on  $L|K$  becomes a problem of finding regular subgroups  $N$  of  $\text{Perm}(G)$  normalized by  $\lambda(G)$ .

If  $L \otimes_K H \cong LN$ , then we say  $H$  has associated group  $N$ .

Subsequently, Byott [By96] translated the problem. Suppose  $N$  is a group of the same cardinality as  $G$ , and let  $\text{Hol}(N) \subset \text{Perm}(N)$  be the normalizer of  $\lambda(N)$ . Then  $\text{Hol}(N) = \rho(N) \cdot \text{Aut}(N)$ , where  $\rho : N \rightarrow \text{Perm}(N)$  is the right regular representation ( $\rho(g)(x) = xg^{-1}$ ). Byott showed that there is a bijection between Hopf Galois structures on  $L|K$  where the  $K$ -Hopf algebra  $H$  has associated group  $N$  and equivalence classes of regular embeddings of  $G$  into  $\text{Hol}(N)$ , where two embeddings  $\beta, \beta' : G \rightarrow \text{Hol}(N)$  are equivalent if there is an automorphism  $\gamma$  of  $N$  so that for all  $\sigma$  in  $G$ ,  $\gamma\beta(\sigma)\gamma^{-1} = \beta'(\sigma)$ .

Let  $e(G, N)$  denote the number of equivalence classes of regular embeddings of  $G$  into  $\text{Hol}(N)$ . Then the number of Hopf Galois structures on  $L|K$  is the sum  $\sum e(G, N)$ , where the sum is over all isomorphism types of groups  $N$  of the same

---

Received by the editors July 1, 2010 and, in revised form, August 24, 2010 and November 12, 2010.

2010 *Mathematics Subject Classification*. Primary 12F10; Secondary 16N20, 20B25, 16W30.

©2012 American Mathematical Society  
Reverts to public domain 28 years from publication

order as  $G$ . Counting the number of Hopf Galois structures on  $L|K$  then becomes a set of problems, one for each isomorphism type of groups  $N$  of the same cardinality as  $G$ .

It is therefore of interest to know when  $e(G, N) = 0$ . Of course, since  $L|K$  is Galois with Galois group  $G$ ,  $e(G, G) \geq 1$ , and as Greither and Pareigis showed, if  $G$  is not abelian, then  $e(G, G) \geq 2$ . But for  $N$  not isomorphic to  $G$ , there have been some results on this question. For example, Byott [By96] showed that if the order of  $G$  is a Burnside number, then  $e(G, N) = 0$  if  $N$  is not isomorphic to  $G$  and  $= 1$  for  $N = G$ . In [CaC99], respectively [By04], it was shown that if  $G$  is a simple non-abelian group, then  $e(G, N) = 2$ , resp.  $0$ , if  $N$  is, resp. is not, isomorphic to  $G$ . Kohl [Ko98] showed that if  $G$  is cyclic of odd prime power order, then  $e(G, N) = 0$  unless  $N \cong G$ . On the other hand, there are groups  $G$  for which  $e(G, N) \neq 0$  for every group  $N$  of the same cardinality as  $G$ ; see, for example, [Ch03] or Proposition 6.1 of [Ko07].

In this paper we prove that if  $G$  and  $N$  are non-isomorphic abelian  $p$ -groups where  $N$  has  $p$ -rank  $m$  and the prime  $p > m + 1$ , then  $e(G, N) = 0$ . The proof utilizes methods of [CDVS06] that relate abelian regular subgroups of  $\text{Hol}(N)$  to commutative associative nilpotent ring structures on  $N$  (Proposition 2 below).

Following the proof we look at a set of examples that show that the hypotheses on the main theorem are necessary.

For a discussion of the relationship between Hopf Galois structures and local Galois module theory, see [Ch00].

## 2. THE MAIN THEOREM

**Theorem 1.** *Let  $p$  be prime and  $N$  be a finite abelian  $p$ -group of  $p$ -rank  $m$ . If  $m + 1 < p$ , then every regular abelian subgroup of  $\text{Hol}(N)$  is isomorphic to  $N$ .*

Before proceeding to the proof, we make some preliminary observations.

The paper [CDVS06] proves that if  $(N, +)$  is a finite elementary abelian  $p$ -group, then every abelian regular subgroup  $T$  of  $\text{Hol}(N) \cong N \rtimes \text{Aut}(N)$  yields a commutative, associative multiplication  $\cdot$  on  $N$  so that  $(N, +, \cdot)$  is a nilpotent ring, as follows. Define a function  $\tau : N \rightarrow \text{Hol}(N) \subset \text{Perm}(N)$  by:  $\tau(a)$  is the unique element  $b \cdot \alpha$  of  $T$  (for  $b$  in  $N$ ,  $\alpha$  in  $\text{Aut}(N)$ ) such that  $\tau(a)(0) = a$ . (Since  $\alpha(0) = 0$  and  $b(0) = 0 + b$ , necessarily  $b = a$ .) Write  $\alpha(x) = x + \delta(x)$  for all  $x$  in  $N$ . Then  $\delta : N \rightarrow N$  is a homomorphism of  $(N, +)$  and defines a multiplication on  $N$  by  $a \cdot b = \delta(a)(b)$ . This multiplication is commutative and associative and makes  $(N, +, \cdot)$  into a nilpotent ring. It then follows from [Ja65, p. 4] that the operation

$$a \circ b = a + b + a \cdot b$$

makes  $(N, \circ)$  into an abelian group, and the function  $\tau : N \rightarrow T$  yields an isomorphism from  $(N, \circ)$  to  $T$ .

It is straightforward to verify that the argument of Theorem 1 of [CDVS06] extends without change to the case where  $N$  is an arbitrary finite abelian  $p$ -group to give

**Proposition 2.** *Let  $(N, +)$  be a finite abelian  $p$ -group. Then each regular abelian subgroup of  $\text{Hol}(N)$  is isomorphic to the group  $(N, \circ)$  induced from a structure  $(N, +, \cdot)$  of a commutative, associative nilpotent ring on  $(N, +)$ , where  $a \circ b = a + b + a \cdot b$ .*

We will use this description of regular abelian subgroups of  $\text{Hol}(N)$ .

*Notation.* For  $m > 0$  and  $a$  in  $N$ , define  $m_{\circ}a = a \circ a \circ \dots \circ a$  ( $m$  factors).

The following easily verified formula is a key to the proof of the main theorem:

**Lemma 3.** For  $a$  in  $(N, +)$ ,

$$p_{\circ}a = pa + \sum_{i=2}^{p-1} \binom{p}{i} a^i + a^p.$$

As a first simple example of how Lemma 3 will be exploited, we prove a slightly stronger version of Theorem 1 in the elementary abelian case.

**Proposition 4.** Let  $p$  be prime and  $N$  be a finite elementary abelian  $p$ -group of  $p$ -rank  $m$ . If  $m < p$ , then every regular abelian subgroup of  $\text{Hol}(N)$  is isomorphic to  $N$ .

*Proof.* Since  $(N, +, \cdot)$  is a nilpotent ring of order  $p^m$  and  $p \geq m + 1$ , we have  $N^p \subseteq N^{m+1} = \{0\}$ , so that  $a^p = 0$  for all  $a$  in  $N$ . Now Lemma 3 implies immediately that  $(N, \circ)$  is also elementary abelian.  $\square$

### 3. PROOF OF THE MAIN THEOREM

For  $i \geq 0$ , let

$$\Omega_i(N, +) = \{x \in N \mid p^i x = 0\}.$$

If  $(N, +)$  has exponent  $p^e$ , we have

$$0 \subset \Omega_1(N, +) \subset \dots \subset \Omega_e(N, +) = N.$$

Each  $\Omega_i(N, +)$  is an ideal of  $(N, +, \cdot)$ , hence also a subgroup of  $(N, \circ)$ .

Similarly, for  $i \geq 0$ , let

$$\Omega_i(N, \circ) = \{x \in N \mid p_{\circ}^i x = 0\}.$$

The core of the proof is to show that  $(N, +)$  and  $(N, \circ)$  have the same number of elements of each order.

**Proposition 5.** For all  $i \geq 0$ ,

$$\Omega_{i+1}(N, +) \setminus \Omega_i(N, +) \subseteq \Omega_{i+1}(N, \circ) \setminus \Omega_i(N, \circ).$$

Since  $N$  is the disjoint union of  $\{0\}$  and the left (resp. right) sides, we must have equality. It follows that  $(N, +) \cong (N, \circ)$ , proving the main theorem.

*Proof of Proposition 5.* We first do the case  $i = 0$ .

Let  $a \neq 0$  in  $\Omega_1(N, +)$ . Then  $pa = 0$ , so by Lemma 3,

$$p_{\circ}a = a^p.$$

Since  $M = \Omega_1(N, +)$  is an elementary abelian subgroup of  $(N, +)$ , the  $p$ -rank of  $M$  is  $\leq m$ , the  $p$ -rank of  $(N, +)$ . Since  $M$  is an ideal of the nilpotent ring  $(N, +, \cdot)$ ,  $M$  is a nilpotent ring of order dividing  $p^m$ . Since  $m + 1 < p$ ,  $M^p = 0$ . Thus  $a^p = 0$ , and so  $p_{\circ}a = 0$ . Therefore,

$$\Omega_1(N, +) \subset \Omega_1(N, \circ).$$

Now let  $i \geq 0$  and assume by induction that

$$\Omega_i(N, +) \setminus \Omega_{i-1}(N, +) \subset \Omega_i(N, \circ) \setminus \Omega_{i-1}(N, \circ).$$

We prove that

$$\Omega_{i+1}(N, +) \setminus \Omega_i(N, +) \subset \Omega_{i+1}(N, \circ) \setminus \Omega_i(N, \circ).$$

Let  $a \in \Omega_{i+1}(N, +) \setminus \Omega_i(N, +)$ .

We first show that  $a$  is in  $\Omega_{i+1}(N, \circ)$ .

If  $a$  is in  $\Omega_{i+1}(N, +)$ , then  $pa$  is in  $\Omega_i(N, +)$ . Now

$$p \circ a = pa + \sum_{i=2}^{p-1} \binom{p}{i} a^i + a^p,$$

so  $p \circ a$  is in  $\Omega_i(N, +)$  iff  $a^p$  is in  $\Omega_i(N, +)$ . But  $M = \Omega_{i+1}(N, +) / \Omega_i(N, +)$  is an elementary abelian section of  $(N, +)$ , hence has  $p$ -rank  $\leq m$ , and so  $|M| \leq p^m$ . Also,  $M$  is the quotient of two ideals of  $(N, +, \cdot)$ , hence is nilpotent. Thus  $M^{m+1} = 0$ . Since  $m + 1 < p$ , we have  $M^p = 0$ . Thus  $a^p$  is in  $\Omega_i(N, +)$ , hence  $p \circ a$  is in  $\Omega_i(N, +) \subset \Omega_i(N, \circ)$ . Thus  $a$  is in  $\Omega_{i+1}(N, \circ)$ .

Now we show that  $a$  is not in  $\Omega_i(N, \circ)$ , by showing that  $p \circ a$  is not in  $\Omega_{i-1}(N, +)$ . Then  $p \circ a$  is in  $\Omega_i(N, +) \setminus \Omega_{i-1}(N, +) \subset \Omega_i(N, \circ) \setminus \Omega_{i-1}(N, \circ)$ , and hence  $a$  is not in  $\Omega_i(N, \circ)$ .

To show that  $p \circ a$  is not in  $\Omega_{i-1}(N, +)$  we look at the subring  $S$  of  $\Omega_{i+1}(N, +) / \Omega_{i-1}(N, +)$  generated by  $a$ . Then  $S$  is a nilpotent subring of  $(N, +, \cdot)$ , and we have a decreasing chain

$$S \supset S^2 \supset \dots$$

Now  $pa$  is not in  $\Omega_{i-1}(N, +)$ , so  $pa \neq 0$  in  $S$ . Recall Lemma 3:

$$p \circ a = pa + \sum_{i=2}^{p-1} \binom{p}{i} a^i + a^p.$$

If  $pa$  is not in  $S^2$ , then  $pa \equiv p \circ a \pmod{S^2}$ , so  $p \circ a \neq 0$  in  $S$ , and hence  $p \circ a$  is not in  $\Omega_{i-1}(N, +)$ .

Suppose  $pa$  is in  $S^k$  and not in  $S^{k+1}$  for some  $k > 1$ . Then  $S/S^k \subset S/pS$  is an elementary abelian section of  $(N, +)$ , so has  $p$ -rank  $\leq m$ . Also,  $S/S^k$  is an  $\mathbb{F}_p$ -vector space with basis  $a, a^2, \dots, a^{k-1}$ . Hence  $k - 1 \leq m < p - 1$ , and so  $k + 1 \leq p$ . Thus  $a^p$  is in  $S^{k+1}$ . Looking again at Lemma 3, we see that  $p \circ a \equiv pa \pmod{S^{k+1}}$ . Thus  $p \circ a$  is in  $\Omega_i(N, +)$  but not in  $\Omega_{i-1}(N, +)$ , and hence in  $\Omega_i(N, \circ) \setminus \Omega_{i-1}(N, \circ)$ . Therefore  $a$  is in  $\Omega_{i+1}(N, \circ) \setminus \Omega_i(N, \circ)$ . Thus

$$\Omega_{i+1}(N, +) \setminus \Omega_i(N, +) \subset \Omega_{i+1}(N, \circ) \setminus \Omega_i(N, \circ).$$

By induction, the proof of Proposition 5 is complete, proving the main theorem.  $\square$

*Remark 6.* If  $N$  is an elementary abelian  $p$ -group, then  $\text{Hol}(N) \equiv \text{AGL}(N)$ , the affine group of the  $\mathbb{F}_p$ -vector space  $N$ , that is, the semidirect product  $N \rtimes \text{Aut}(N)$ . If  $N$  has dimension  $m$ , then  $\text{Aut}(N)$  may be viewed as the matrix group  $\text{GL}_m(\mathbb{F}_p)$ . It is perhaps worth observing that that description may be generalized. Suppose

$$N = Z_p^{n_1} \times Z_p^{n_2} \times \dots \times Z_p^{n_m},$$

where  $n_1 \leq n_2 \leq \dots \leq n_m$ . Then we may view endomorphisms of  $N$  as matrices of homomorphisms of the indecomposable direct factors of  $N$ . If  $A$  is an endomorphism of  $N$ , then  $A$  may be written as

$$A = \begin{pmatrix} f_{11} & \cdots & f_{m1} \\ \vdots & & \vdots \\ f_{1m} & \cdots & f_{mm} \end{pmatrix},$$

where  $f_{ij}$  is a homomorphism from  $\mathbb{Z}/p^{n_i}\mathbb{Z}$  to  $\mathbb{Z}/p^{n_j}\mathbb{Z}$ . Now

$$\begin{aligned} \text{Hom}(\mathbb{Z}/p^{n_i}\mathbb{Z}, \mathbb{Z}/p^{n_j}\mathbb{Z}) \\ \cong p^{n_j-n_i}(\mathbb{Z}/p^{n_j}\mathbb{Z}) \text{ if } n_j \geq n_i \\ \cong \mathbb{Z}/p^{n_j}\mathbb{Z} \text{ if } n_j \leq n_i. \end{aligned}$$

Thus given the “standard” basis  $\{e_1, \dots, e_m\}$  of  $N$ , namely,

$$e_1 = (1, 0, \dots, 0)^{tr}, \dots, e_m = (0, \dots, 0, 1)^{tr},$$

we can associate a matrix of integers to the endomorphism  $A$  as follows: let

$$\begin{aligned} f_{ij}(e_i) &= p^{n_j-n_i}a_{i,j}e_j \text{ if } i \leq j \\ &= a_{ij}e_j \text{ if } i \geq j, \end{aligned}$$

where  $a_{ij}$  in both cases is defined modulo  $p^{n_j}$ . Then the matrix of  $A$  relative to the standard basis is

$$\mathbf{A} = \begin{pmatrix} a_{1,1} & a_{2,1} & \cdots & a_{m,1} \\ p^{n_2-n_1}a_{1,2} & a_{2,2} & \cdots & a_{m,2} \\ \vdots & & & \vdots \\ p^{n_m-n_1}a_{1,m} & p^{n_m-n_2}a_{2,m} & \cdots & a_{m,m} \end{pmatrix},$$

where the entries in the  $j$ th row are defined modulo  $p^{n_j}$ .

Following Hillar and Rhea [HR07], let  $R_p$  be the set of all matrices in  $M_m(\mathbb{Z})$  of the form  $\mathbf{A}$  as above, where all  $a_{i,j}$  are in  $\mathbb{Z}$ . Then  $R_p$  is a ring with identity under matrix multiplication ([HR07], (3.2)), and the map

$$\psi : R_p \rightarrow \text{End}(N)$$

given by  $(b_{i,j}) \mapsto (b_{i,j} \bmod p_j)$  is a surjective homomorphism ([HR07], (3.3)). If  $\pi : \text{End}(N) \rightarrow \text{End}((\mathbb{Z}/p\mathbb{Z})^m)$  is the map induced by mapping the matrix  $\mathbf{A} = (a_{i,j})$  in  $R_p$  (or equivalently,  $\psi(\mathbf{A})$  in  $\text{End}(N)$ ) to  $\pi(\mathbf{A}) = (a_{i,j} \bmod p)$ , then  $\psi(\mathbf{A})$  is an automorphism of  $N$  iff  $\pi(\mathbf{A})$  is in  $\text{GL}_m((\mathbb{Z}/p\mathbb{Z}))$  ([HR07], (3.6)).

A proof of the main theorem (with a somewhat more restrictive hypothesis on  $p$ ) may be constructed using this description of  $\text{Hol}(N)$ ; see [Fe03].

#### 4. EXAMPLES

We first give examples showing that the condition  $m < p$  in Proposition 4 is necessary.

**Example 7.** We find an example of a regular abelian subgroup  $G$  of  $\text{Hol}((\mathbb{Z}/3\mathbb{Z})^3)$  of exponent 9. Since  $\mathbb{Z}/3\mathbb{Z} \rtimes U_3(\mathbb{Z}/3\mathbb{Z})$  is a 3-Sylow subgroup of  $\text{Hol}((\mathbb{Z}/3\mathbb{Z})^3)$  and

is isomorphic to  $U_4(\mathbb{Z}/3\mathbb{Z})$  under the embedding of  $\text{Hol}(\mathbb{Z}/3\mathbb{Z})$  into  $\text{GL}_4(\mathbb{Z}/3\mathbb{Z})$ , it suffices to find a regular subgroup of exponent 9 in  $U_4(\mathbb{Z}/3\mathbb{Z})$ .

Let

$$S = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then

$$S^3 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

so  $S$  has order 9. It is routine to verify that  $T$  has order 3 and  $S$  and  $T$  commute, so  $G = \langle S, T \rangle$  is an abelian subgroup of  $U_4(\mathbb{Z}/3\mathbb{Z})$  of order 27. To check regularity we need to show that the map  $\pi : G \rightarrow \mathbb{Z}/3\mathbb{Z}$  given by

$$\pi\left(\begin{pmatrix} 1 & * & * & a \\ 0 & 1 & * & b \\ 0 & 0 & 1 & c \\ 0 & 0 & 0 & 1 \end{pmatrix}\right) \rightarrow (a, b, c)$$

is onto. But we may verify easily that

$$\pi(S^c) = (x, y, c)$$

for some  $x, y$  in  $\mathbb{Z}/3\mathbb{Z}$ , and then for any matrix  $M$  in  $U_4(\mathbb{Z}/3\mathbb{Z})$ , if  $\pi(M) = (a, b, c)$ , then

$$\pi(TM) = (a + c, b + 1, c) \text{ and } \pi(S^3M) = (a + 1, b, c).$$

Hence given  $(a, b, c)$  in  $(\mathbb{Z}/3\mathbb{Z})^3$ , we have  $\pi(S^c) = (x, y, c)$  for some  $x, y$  in  $\mathbb{Z}/3\mathbb{Z}$ . Then  $\pi(T^{b-y}S^c) = (w, b, c)$  for some  $w$ , and then  $\pi(S^{3(a-w)}T^{b-y}S^c) = (a, b, c)$ . So  $G$  is a regular subgroup of  $\text{Hol}((\mathbb{Z}/3\mathbb{Z})^3)$  but is not isomorphic to  $(\mathbb{Z}/3\mathbb{Z})^3$ .

**Example 8.** Let  $F = \mathbb{F}_p$ , let  $R$  be the truncated polynomial ring  $F[x]/x^{m+1}F[x]$ , and let  $N = xF[x]/x^{m+1}F[x]$ , a nilpotent subring of  $R$ . Then  $(N, +)$  is an elementary abelian  $p$ -group of rank  $m$ . With the operation  $u \circ v = u + v + u \cdot v$ ,  $(N, \circ)$  is an abelian regular subgroup of  $\text{Hol}(N, +)$ . The map  $u \mapsto 1 + u$  defines an isomorphism from  $(N, \circ)$  onto the group  $U_1(R)$  of principal units of  $R$ .

Let  $m = p$  and  $a$  be the image of  $x$  in  $R$ . Then, using Lemma 3, we have

$$p \circ a = \sum_{i=1}^{p-1} \binom{p}{i} a^i + a^p = a^p \neq 0,$$

so that  $(N, \circ)$  has exponent at least  $p^2$ . In fact, in [Ch07], Corollary 3, the structure of  $(N, \circ) \cong U_1(R)$  as an abelian  $p$ -group was determined for every  $m$ : for  $m = p$ ,  $(N, \circ)$  has type  $(p^2, p, \dots, p)$  (i.e.,  $(N, \circ) \cong Z_{p^2} \times Z_p^{p-1}$ ).

Here is a “reverse” of the last example. This example shows that the condition  $m + 1 < p$  in Theorem 1 is necessary.

**Example 9.** Let  $S$  be the ring  $x\mathbb{Z}[x]/x^{p+1}\mathbb{Z}[x]$ , let  $\bar{x}$  be the image of  $x$  in  $S$ , let  $(N, +, \cdot) = S/(p\bar{x} + \bar{x}^p)S$ , and let  $a$  be the image of  $\bar{x}$  in  $N$ . Then

$$(1) \quad pa + a^p = 0, a^{p+1} = 0 \text{ and } pa^i = 0 \text{ for } i > 1.$$

Thus  $(N, +)$  has generators  $a, a^2, \dots, a^{p-1}$  with  $pa = -a^p \neq 0$ , so  $(N, +)$  has order  $p^p$ ,  $p$ -rank  $m = p - 1$  and type  $(p^2, p, \dots, p)$ .

Since  $(N, +, \cdot)$  is a nilpotent ring, the operation  $u \circ v = u + v + u \cdot v$  for  $u, v$  in  $N$  defines a group  $(N, \circ)$ , which by Proposition 2 is isomorphic to an abelian regular subgroup of  $\text{Hol}(N, +)$ . Using Lemma 3 and the relations (1), we have

$$p \circ a = pa + \sum_{i=2}^{p-1} \binom{p}{i} a^i + a^p = 0,$$

so that  $(N, \circ)$  is elementary abelian.

Now we give an example to show that the abelian assumption is necessary.

**Example 10.** Let  $p \geq 5$ , let  $N = \mathbb{F}_p^3$  and let

$$G = U_3(\mathbb{F}_p) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{F}_p \right\}.$$

Then  $G$  is a non-abelian group in which every element of  $G$  has order dividing  $p$ . We show that  $G$  has a regular embedding in  $\text{Hol}(N)$ .

Evidently  $G = \langle A, B, C \rangle$  with

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

with  $C$  central in  $G$  and  $A, B$  satisfying  $AB = CBA$ .

Identify the  $p$ -Sylow subgroup of  $\text{Hol}(\mathbb{F}_p^3)$  with  $U_4(\mathbb{F}_p)$  as in Example 7, and let  $\beta : G \rightarrow U_4(\mathbb{F}_p)$  be given by

$$\beta(A) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \beta(B) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$\beta(C) = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

One may verify that  $\beta$  is a homomorphism and that an element of  $\beta(G)$  has the form

$$\beta(A^r B^s C^t) = \begin{pmatrix} 1 & q & \binom{q}{2} & x \\ 0 & 1 & q & s + \binom{q}{2} \\ 0 & 0 & 1 & q \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

where  $q = r + s$  and  $x = w + t$  and where  $w$  depends only on  $r$  and  $s$ .

To show that the group  $\beta(G)$  is regular, we need to show that the map  $\pi : U_4(\mathbb{F}_p) \rightarrow \mathbb{F}_p^3$  given by

$$\pi(\beta(A^r B^s C^t)) = (w + t, s + \binom{r + s}{2}, r + s)$$

is onto, that is, for all  $(a, b, c)$  in  $\mathbb{F}_p^3$ , there exist  $r, s, t$  so that

$$\begin{aligned} a &= w + t, \\ b &= s + \binom{r + s}{2}, \\ c &= r + s. \end{aligned}$$

But  $b = s + \binom{c}{2}$  determines  $s$ , then  $c = r + s$  determines  $r$ , hence  $w$ , and then  $w + t = a$  determines  $t$ . So  $\beta(G)$  is a (non-abelian) regular subgroup of  $\text{Hol}(\mathbb{Z}/p\mathbb{Z}^3)$ .

*Remark 11.* Recall that  $e(G, N)$  is the number of  $H$ -Hopf Galois structures on a Galois extension of fields with Galois group  $G$ , where the Hopf algebra  $H$  has associated group  $N$ . When  $e(G, N) > 0$  it is of interest to determine  $e(G, N)$ , or at least to find a lower bound for  $e(G, N)$ .

For  $N$  an elementary abelian  $p$ -group of rank  $m$  with  $p > m$ , a lower bound for  $e(N, N)$  was found in [Ch05]. If  $p \geq 5$  and  $G$  is the group of principal units of the ring  $\mathbb{F}_p[x]/(x^{m+1})$  as in Example 8, a lower bound for  $e(G, N)$  was found in [Ch07], namely,  $e(G, N) > p^{(m+1)^2/3-m}$ .

Continuing with Example 10, we have

**Proposition 12.** *Let  $N$  be an elementary abelian  $p$ -group of rank 3 with  $p \geq 5$  and let  $G = U_3(\mathbb{F}_p)$ . Then there are  $p^3 - p$   $H$ -Hopf Galois structures on a Galois extension of fields with Galois group  $G$ , where  $H$  has associated group  $N$ .*

*Proof.* Following the approach in [Ch07], we can determine  $e(G, N)$  by determining  $\text{Aut}(G)$  and the stabilizer  $\text{Sta}(J)$  in  $\text{Aut}(N)$  of the subgroup  $J = \beta(G)$  inside  $U_4(\mathbb{F}_p)$ ; then  $e(G, N) = |\text{Aut}(G)|/|\text{Sta}(J)|$ .

We first find  $\text{Aut}(G)$ .

Since every element of  $G$  has order dividing  $p$  and the center of  $G$  is generated by  $C$ , an endomorphism  $\alpha$  of  $G$  satisfies

$$\alpha(A) = A^r B^s C^t, \quad \alpha(B) = A^x B^y C^z, \quad \alpha(C) = C^c,$$

where since  $AB = CBA$ , we must have

$$c = sx - ry = \det \begin{pmatrix} s & y \\ r & x \end{pmatrix}.$$

If  $\alpha(A^l B^m C^n) = 1$ , then

$$(A^r B^s C^t)^l (A^x B^y C^z)^m (C^c)^n = 1.$$

This has the form

$$A^{r^l + xm} B^{s^l + ym} C^k$$

for some  $k$  (all exponents in  $\mathbb{F}_p$ ). If  $c \neq 0$ , then  $\det \begin{pmatrix} s & y \\ r & x \end{pmatrix} \neq 0$ ; hence  $\alpha(A^l B^m C^n) = 1$  only for  $l, m, n = 0$ . Thus  $\alpha$  is an automorphism for all  $r, s, t, x, y, z, c$  such that



$c = sx - ry \neq 0$ . Since  $t$  and  $z$  may be chosen arbitrarily,

$$|\text{Aut}(G)| = |\mathbb{Z}/p\mathbb{Z}|^2 \cdot |\text{GL}_2(\mathbb{Z}/p\mathbb{Z})| = p^2(p^2 - 1)(p^2 - p).$$

As for  $\text{Sta}(J)$ , it is a subgroup of

$$\begin{pmatrix} \text{GL}_3(\mathbb{Z}/p\mathbb{Z}) & 0 \\ 0 & 1 \end{pmatrix} \subset \text{GL}_4(\mathbb{Z}/p\mathbb{Z}).$$

For  $\begin{pmatrix} P & 0 \\ 0 & 1 \end{pmatrix}$  in  $\text{Sta}(J)$ , the equation

$$\begin{pmatrix} P & 0 \\ 0 & 1 \end{pmatrix} \beta(A) = \beta(A^r B^s C^t) \begin{pmatrix} P & 0 \\ 0 & 1 \end{pmatrix}$$

for some  $r, s, t$  implies that  $P$  has the form

$$P = \begin{pmatrix} q^3 & eq + q\binom{q}{2} & c \\ 0 & q & e \\ 0 & 0 & q \end{pmatrix},$$

where  $q = r + s \neq 0$  and  $e = s + \binom{q}{2}$  and  $c$  is an arbitrary element of  $\mathbb{F}_p$ , and conversely, if  $P$  has that form, then  $\begin{pmatrix} P & 0 \\ 0 & 1 \end{pmatrix}$  is in  $\text{Sta}(J)$ . Hence  $|\text{Sta}(J)| = p^2(p-1)$ , and so

$$e(G, N) = |\text{Aut}(G)|/|\text{Sta}(J)| = p^3 - p. \quad \square$$

REFERENCES

[By96] N. P. Byott, Uniqueness of Hopf Galois structure of separable field extensions, *Comm. Algebra* 24 (1996), 3217–3228. MR1402555 (97j:16051a)

[By04] N. P. Byott, Hopf-Galois structures on field extensions with simple Galois groups, *Bull. London Math. Soc.* 36 (2004), 45–57. MR2011974 (2004i:16049)

[CDVS06] A. Caranti, F. Dalla Volta, M. Sala, Abelian regular subgroups of the affine group and radical rings, *Publ. Math. Debrecen* 69 (2006), 297–308. MR2273982 (2007j:20001)

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

[CS69] S. U. Chase, M. E. Sweedler, Hopf algebras and Galois theory, *Lecture Notes in Mathematics*, Vol. 97, Springer-Verlag, Berlin-New York, 1969. MR0260724 (41:5348)

[Ch00] L. N. Childs, *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory*, *Mathematical Surveys and Monographs* 80, American Mathematical Society, 2000. MR1767499 (2001e:11116)

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

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

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

[Fe03] S. C. Featherstonhaugh, Abelian Hopf Galois extensions on Galois field extensions of prime power order, Ph.D. thesis, Univ. at Albany, NY, 2003.

[GP87] C. Greither, B. Pareigis, Hopf Galois theory for separable field extensions, *J. Algebra* 106 (1987), 239–258. MR878476 (88i:12006)

[HR07] C. Hillar, D. Rhea, Automorphisms of finite abelian groups, *Amer. Math. Monthly* 114 (2007), 917–923. MR2363058

[Ja65] N. Jacobson, *Structure of Rings*, 2nd. ed., Amer. Math. Soc. Colloq. 37, 1965. MR0044505 (13:426f)

- [Ko98] T. Kohl, Classification of the Hopf Galois structures on prime power radical extensions, *J. Algebra* 207 (1998), 525–546. MR1644203 (99g:16049)
- [Ko07] T. Kohl, Groups of order  $4p$ , twisted wreath products and Hopf-Galois theory, *J. Algebra* 314 (2007), 42–74. MR2331752 (2008e:12001)

DEPARTMENT OF MATHEMATICS, BOROUGH OF MANHATTAN COMMUNITY COLLEGE/CUNY, 199 CHAMBERS STREET, ROOM N-520, NEW YORK, NEW YORK 10007

*E-mail address:* `sfeatherstonhaugh@bmcc.cuny.edu`

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DEGLI STUDI DI TRENTO, VIA SOMMARIVE 14, I-38123 TRENTO, ITALY

*E-mail address:* `caranti@science.unitn.it`

DEPARTMENT OF MATHEMATICS, UNIVERSITY AT ALBANY, ALBANY, NEW YORK 12222

*E-mail address:* `lchilds@albany.edu`