New York Journal of Mathematics

New York J. Math. **18** (2012) 707–731.

Fixed-point free pairs of homomorphisms and nonabelian Hopf–Galois structures

Nigel P. Byott and Lindsay N. Childs

Abstract. Given finite groups Γ and G of order n, regular embeddings from Γ to the holomorph of G yield Hopf–Galois structures on a Galois extension $L|K$ of fields with Galois group Γ. Here we consider regular embeddings that arise from fixed-point free pairs of homomorphisms from Γ to G. If G is a complete group, then all regular embeddings arise from fixed-point free pairs. For all Γ, G of order $n = p(p-1)$ with p a safeprime, we compute the number of Hopf–Galois structures that arise from fixed-point free pairs, and compare the results with a count of all Hopf–Galois structures obtained by T. Kohl. Using the idea of fixed-point free pairs, we characterize the abelian Galois groups Γ of even order or order a power of p, an odd prime, for which $L|K$ admits a nonabelian Hopf Galois structure. The paper concludes with some new classes of abelian groups Γ for which every Hopf–Galois structure has type Γ (and hence is abelian).

Contents

Received March 17, 2012.
2010 *Mathematics Subject Classification.* 12F10 (primary), 16W30 (secondary).
Key words and phrases. Hopf–Galois structure; abelian extensions; semidirect product.

ISSN 1076-9803/2012

1. Introduction

Let L be a Galois extension of K, fields, with Galois group Γ of order n. Let H be a K-Hopf algebra acting on L so that L is an H-module algebra. Then $L|K$ is an H-Hopf–Galois extension if the natural map $L \otimes_K H \to \mathrm{End}_K(L)$ is bijective. A Hopf–Galois structure on $L|K$ is an action of a K-Hopf algebra H on L making $L|K$ into an H-Hopf–Galois extension. (In contrast to the Hopf algebra $H = K[\Gamma]$, it is possible for a K-Hopf algebra H to have more than one Hopf–Galois structure on $L|K$: see, e.g., [CCo07].)

Greither and Pareigis [GP87] showed that Hopf–Galois structures on $L|K$ are in one–to-one correspondence with regular subgroups of $\mathrm{Perm}(\Gamma)$ normalized by $\lambda(\Gamma)$, the image in $\mathrm{Perm}(\Gamma)$ of the left regular representation $\lambda : \Gamma \to \mathrm{Perm}(\Gamma)$ given by $\lambda(\sigma)(x) = \sigma x$. The idea is that if $L|K$ is a Galois extension with Galois group Γ, then $L \otimes_K L \cong \mathrm{Hom}(\Gamma, L) = \sum_{\sigma\in\Gamma} Le_\sigma$ where $\{e_\sigma : \sigma \in \Gamma\}$ is the dual basis to the basis Γ of LG. If $L|K$ is also an H-Hopf–Galois extension for some K-Hopf algebra H, then $L \otimes_K H = LM$ where the group M permutes the dual basis, hence may be viewed as a regular subgroup of $\mathrm{Perm}(\Gamma)$ that is normalized by $\lambda(\Gamma)$.

Conversely, if M is a regular subgroup of $\mathrm{Perm}(\Gamma)$ acting on the subscripts of the dual basis, then $L \otimes_K L$ is acted on by the L-Hopf algebra LM, making $L \otimes_K L$ into an LM-Hopf–Galois extension of L: if M is normalized by $\lambda(\Gamma)$, then $H = (LM)^\Gamma$ is a K-Hopf algebra, $(L \otimes_K L)^\Gamma \cong L$ and the action of LM on $L \otimes_K L$ descends by Galois descent to an action of H on L making $L|K$ an H-Galois extension of L.

Thus finding, or at least counting, Hopf–Galois structures on a Galois extension $L|K$ of fields with Galois group Γ is transformed into a problem in finite groups.

If $L|K$ is an H-Hopf–Galois extension of order n, G is an abstract group of order n and $L \otimes_K H \cong LG$, we say that H has *type* G.

For G a finite group, $\mathrm{Hol}(G)$, the holomorph of G, is the normalizer in $\mathrm{Perm}(G)$ of $\lambda(G)$. Then $\mathrm{Hol}(G) = \rho(G) \cdot \mathrm{Aut}(G)$, where $\rho : G \to \mathrm{Perm}(G)$ is the right regular representation, $\rho(\sigma)(x) = x\sigma^{-1}$. Clearly $\lambda(G) \subset \mathrm{Hol}(G)$, and $\lambda(G)$ and $\rho(G)$ centralize each other. So $\lambda(G) \cdot \rho(G) \subset \mathrm{Hol}(G)$.

For G an abstract group of order n, let $R(\Gamma, [G])$ be the set of regular subgroups M of $\mathrm{Perm}(\Gamma)$ that are isomorphic to G and normalized by $\lambda(\Gamma)$. From [By96] or Section 7 of [Ch00] one knows that $R(\Gamma, [G])$ is bijective with the set of regular embeddings β of Γ into $\mathrm{Hol}(G)$ modulo the equivalence: $\beta \sim \beta'$ if there exists δ in $\mathrm{Aut}(G)$ so that for all σ in Γ, $\beta'(\sigma) = \delta\beta(\sigma)\delta^{-1}$.

In this paper, as with most papers in this subject, we determine the number of Hopf–Galois structures on $L|K$ with Galois group Γ, or at least a lower bound on that number, by the above bijection: we look for equivalence classes of regular embeddings of Γ into $\mathrm{Hol}(G)$ for groups G of the same cardinality as Γ.

Using this bijection, several papers over the past dozen years have obtained Hopf–Galois structures from fixed-point free endomorphisms of Γ, the

Galois group of $L|K$. See, for example, [CaC99], [Ch03], [CCo07], [Ch11]. In all cases, the resulting Hopf–Galois structures involve a K-Hopf algebra H of type Γ. Here we extend this strategy to look at fixed-point free pairs of homomorphisms from a group Γ to a group G of the same finite cardinality, and use such pairs to obtain Hopf–Galois structures where the type G of the Hopf algebra is not necessarily isomorphic to the Galois group Γ.

In Sections 3 and 4 we explore the applicability of the method of fixed-point free pairs. For groups of order $p(p-1)$ where p is a safeprime, we compare the counts with counts of all Hopf–Galois structures on Galois extensions with such Galois groups in [Ch03] and [Ko11]. If Γ is cyclic of order pq with q dividing $p-1$, then all of the $2q-1$ Hopf–Galois structures on a Galois extension with Galois group Γ found in [By04] arise from fixed-point free pairs of homomorphisms.

A simple application of fixed-point free pairs is from the direct product of two groups to a semidirect product of the two groups. Using that observation, we show in Section 5 that "most" Galois extensions $L|K$ with a noncyclic abelian Galois group Γ have nonabelian Hopf–Galois structures. In particular, we may characterize the Galois extensions with nonabelian Hopf–Galois structures where the Galois group Γ is abelian of order that is even or a power of p, an odd prime. For abelian Galois groups of odd order divisible by at least two distinct primes we find a large class of examples for which there are nonabelian Hopf–Galois structures.

On the other hand, we find some new classes of abelian groups Γ, of odd order divisible by two distinct primes, such that there are no nonabelian Hopf–Galois structures on a Galois extension with group Γ (and indeed all Hopf–Galois structures are of type Γ), even though nonabelian groups of order $|\Gamma|$ exist.

The second author thanks Tim Kohl for numerous discussions related to this material.

2. Fixed-point free pairs

Let Γ and G be finite groups of the same cardinality.

Definition. Let f and g be homomorphisms from Γ to G. Then (f, g) is a fixed-point free pair of homomorphisms, or for short, an fpf pair, if for all σ in Γ, $f(\sigma) = g(\sigma)$ implies $\sigma = e$, the identity element of Γ.

Proposition 1. *If (f, g) is a fpf pair of homomorphisms from Γ to G, then*

$$\{f(\sigma)g(\sigma^{-1}) : \sigma \in \Gamma\} = G.$$

Proof. If the conclusion is false, then by a cardinality argument there must be $\sigma \neq \tau$ in Γ so that

$$f(\sigma)g(\sigma^{-1}) = f(\tau)g(\tau^{-1}).$$

Then

$$f(\tau^{-1}\sigma) = g(\tau^{-1}\sigma).$$

The element $\pi = \tau^{-1}\sigma$ is not the identity element of Γ and $f(\pi) = g(\pi)$, so (f, g) is not a fpf pair. □

A subgroup N of $\mathrm{Perm}(G)$ is regular if N and G have the same cardinality and $N \cdot e = G$, where e is the identity element of the set G. For Γ a group of the same cardinality as G, a homomorphism $\beta : \Gamma \to \mathrm{Perm}(G)$ is a regular embedding if $\beta(\Gamma)$ is a regular subgroup of $\mathrm{Perm}(G)$.

Recall that $\lambda(G) \cdot \rho(G)$ is a subgroup of $\mathrm{Hol}(G)$. Thus given a fixed-point free pair (f, g) of homomorphisms from Γ to G, we define an embedding $\beta_{(f,g)} : \Gamma \to \mathrm{Hol}(G)$ by

$$\beta_{(f,g)}(\sigma) = \lambda(f(\sigma))\rho(g(\sigma)).$$

Then $\beta_{(f,g)}$ is a homomorphism since $\lambda(G)$ and $\rho(G)$ centralize each other in $\mathrm{Perm}(G)$. By Proposition 1, if (f, g) is a fpf pair, then

$$\begin{aligned}\beta_{(f,g)}(\Gamma) \cdot e &= \{\lambda(f(\sigma))\rho(g(\sigma))(e) | \sigma \in \Gamma\} \\ &= \{f(\sigma)g(\sigma^{-1}) | \sigma \in \Gamma\} = G,\end{aligned}$$

so $\beta_{(f,g)}$ is a regular embedding.

If the center of G is nontrivial, then the correspondence from pairs (f, g) of fixed-point free homomorphisms from Γ to G to regular embeddings $\beta_{(f,g)} : \Gamma \to \mathrm{Hol}(G)$ is not necessarily one-to-one:

Proposition 2. *Let (f, g) and (f', g') be fixed-point free pairs of homomorphisms from Γ to G. Then the corresponding embeddings $\beta_{(f,g)}, \beta_{(f',g')}$ are equal (as functions) if and only if there exists a homomorphism $\zeta : \Gamma \to Z(G)$, the center of G, so that for all σ in Γ,*

$$f'(\sigma) = \zeta(\sigma)f(\sigma) \quad \textit{and} \quad g'(\sigma) = \zeta(\sigma)g(\sigma).$$

Proof. For all σ in Γ, we have

$$\beta_{(f',g')}(\sigma) = \beta_{(f,g)}(\sigma)$$

iff

$$\lambda(f'(\sigma))\rho(g'(\sigma)) = \lambda(f(\sigma))\rho(g(\sigma))$$

iff

$$\lambda(f(\sigma)^{-1}f'(\sigma)) = \rho(g(\sigma)g'(\sigma)^{-1}).$$

Applying both sides to an element x of the set G gives

$$f(\sigma^{-1})f'(\sigma)x = x(g(\sigma)g'(\sigma^{-1}))^{-1} = xg'(\sigma)g(\sigma^{-1}).$$

In particular, for $x = e$, the identity element of G, we have

$$f(\sigma^{-1})f'(\sigma) = g'(\sigma)g(\sigma^{-1}).$$

Let $\zeta(\sigma) = f(\sigma^{-1})f'(\sigma) = g'(\sigma)g(\sigma^{-1})$. Then $\zeta(\sigma)$ is in the center of G, and for all σ in Γ,

$$f'(\sigma) = f(\sigma)\zeta(\sigma), \qquad g'(\sigma) = g(\sigma)\zeta(\sigma).$$

Since $\zeta(\Gamma) \subseteq Z(G)$, it is easy to see that ζ is a homomorphism.

Conversely, if $\zeta : \Gamma \to Z(G)$ is a homomorphism and (f, g) is a fixed-point free pair of homomorphisms from Γ to G, then $(f \cdot \zeta, g \cdot \zeta)$ is a fixed-point free pair of homomorphisms from Γ to G. Now

$$\begin{aligned}\beta_{(f\cdot\zeta, g\cdot\zeta)}(\sigma) &= \lambda(f(\sigma)\zeta(\sigma))\rho(g(\sigma)\zeta(\sigma)) \\ &= \lambda(f(\sigma))\lambda(\zeta(\sigma)\rho(g(\sigma))\rho(\zeta(\sigma)).\end{aligned}$$

Since $\zeta(\sigma)$ is in the center of G, we have for all x in G,

$$\lambda(\zeta(\sigma))\rho(\zeta(\sigma))(x) = \zeta(\sigma)x\zeta(\sigma)^{-1} = \zeta(\sigma)\zeta(\sigma)^{-1}x = x.$$

Thus

$$\lambda(f(\sigma))\lambda(\zeta(\sigma))\rho(g(\sigma))\rho(\zeta(\sigma)) = \lambda(f(\sigma))\rho(g(\sigma)).$$

So

$$\beta_{(f\cdot\zeta, g\cdot\zeta)} = \beta_{(f,g)}. \qquad \square$$

Proposition 2 implies that if G has trivial center, then the map from fixed-point free pairs to regular embeddings is one-to-one.

We must also deal with the equivalence on regular embeddings.

Definition. Two fixed-point free pairs (f, g) and (f', g') are equivalent, $(f, g) \sim (f', g')$, if $\beta_{(f,g)} \sim \beta_{(f',g')}$.

Proposition 3. *Let (f, g) and (f', g') be fixed-point free pairs of homomorphisms from Γ to G. Then $(f, g) \sim (f', g')$ if and only if there exists an automorphism δ of G and a homomorphism $\zeta : \Gamma \to Z(G)$, the center of G, so that for all σ in Γ,*

$$f'(\sigma) = \delta(f(\sigma))\zeta(\sigma) \text{ and } g'(\sigma) = \delta(g(\sigma))\zeta(\sigma).$$

Proof. Given a fixed-point free pair (f, g) and an automorphism δ of G, then for all x in G,

$$\begin{aligned}\beta_{(\delta f, \delta g)}(\sigma)(x) &= \lambda(\delta(f(\sigma))\rho(\delta(g(\sigma))(x) \\ &= \delta(f(\sigma))x\delta(g(\sigma^{-1})) \\ &= \delta(f(\sigma)\delta^{-1}(x)g(\sigma^{-1})) \\ &= \delta(\lambda(f(\sigma))\rho(g(\sigma))\delta^{-1}(x)) \\ &= \delta\beta_{(f,g)}(\sigma)\delta^{-1}(x),\end{aligned}$$

and so $\beta_{(\delta f, \delta g)} \sim \beta_{(f,g)}$. Hence if $f'(\sigma) = \delta(f(\sigma))\zeta(\sigma), g'(\sigma) = \delta(g(\sigma))\zeta(\sigma)$ for some homomorphism $\zeta : \Gamma \to Z(G)$, then

$$\beta_{(f',g')} = \beta_{(f'\cdot\zeta^{-1}, g'\cdot\zeta^{-1})}$$

by Proposition 2, and

$$\beta_{(f'\cdot\zeta^{-1}, g'\cdot\zeta^{-1})} = \beta_{(\delta f, \delta g)} \sim \beta_{(f,g)}.$$

Conversely, suppose (f, g) and (f', g') are fixed-point free pairs and

$$\beta_{(f,g)} \sim \beta_{(f',g')}.$$

Then there is an automorphism δ of G so that for all σ in Γ,

$$\lambda(f'(\sigma))\rho(g'(\sigma)) = \delta\lambda(f(\sigma))\rho(g(\sigma))\delta^{-1}.$$

Applying the two sides to an element x of G yields

$$f'(\sigma)xg'(\sigma)^{-1} = \delta(f(\sigma))x\delta(g(\sigma)^{-1}),$$

hence

$$x\delta(g(\sigma)^{-1})g'(\sigma) = \delta(f(\sigma)^{-1})f'(\sigma)x.$$

In particular, for $x = e$, we have

$$\delta(g(\sigma)^{-1})g'(\sigma) = \delta(f(\sigma)^{-1})f'(\sigma).$$

Let

$$\zeta(\sigma) = \delta(g(\sigma)^{-1})g'(\sigma) = \delta(f(\sigma)^{-1})f'(\sigma).$$

Then $\zeta(\sigma)$ is in the center of G, and

$$g'(\sigma) = \delta(g(\sigma))\zeta(\sigma), \quad f'(\sigma) = \delta(f(\sigma))\zeta(\sigma).$$

Since $\zeta(\sigma)$ is in the center of G, and f' and $\delta \circ f$ are homomorphisms, ζ is a homomorphism from Γ to $Z(G)$. □

3. Some extremes

As always, Γ and G are groups of the same finite cardinality.

For some groups Γ, G, fixed-point free pairs yield no nontrivial Hopf–Galois structures.

For example, if G is abelian, then fixed-point free pairs of homomorphisms into G yield nothing of interest for Hopf–Galois extensions.

Proposition 4. *Suppose G is abelian. If $\beta : \Gamma \to \mathrm{Hol}(G)$ arises from a fixed-point free pair of homomorphisms, then $\Gamma \cong G$ and β is equivalent to λ.*

Proof. In $\mathrm{Hol}(G)$, $\rho(\sigma) = \lambda(\sigma^{-1})$. If $\beta_{(f,g)} : \Gamma \to \mathrm{Hol}(G)$ arises from a fixed-point free pair, then

$$\{\lambda(f(\sigma))\rho(g(\sigma))(e) | \sigma \in \Gamma\} = \{f(\sigma)g(\sigma^{-1})\} = G$$

and the map $\theta : \Gamma \to G$ by $\theta(\sigma) = f(\sigma)g(\sigma^{-1})$ is a homomorphism since G is abelian. Thus $\Gamma = G$ and θ is an automorphism. Then for x in G,

$$\begin{aligned}\beta_{(f,g)}(\sigma)(x) &= \lambda(f(\sigma)g(\sigma^{-1}))(x)\\ &= \lambda(\theta(\sigma))(x)\\ &= \theta\lambda(\sigma)\theta^{-1}(x).\end{aligned}$$

So $\beta_{(f,g)}$ is equivalent to λ. □

For Γ abelian, λ corresponds to the classical Hopf–Galois structure arising from the Galois group.

For some groups Γ, fixed-point free pairs of homomorphisms into a non-isomorphic group G cannot exist:

Proposition 5. *If Γ is a group with a unique minimal nontrivial normal subgroup, then if G is not isomorphic to Γ, there are no fixed-point free pairs of homomorphisms from Γ to G.*

Proof. Since Γ is not isomorphic to G, then every homomorphism from Γ to G has a nontrivial kernel. If Γ has a unique minimal nontrivial normal subgroup N, then every pair of homomorphisms (f, g) from Γ to G takes all elements of N to the identity of G, and so (f, g) cannot be fixed-point free. □

Examples include $\Gamma = \mathbb{Z}_{p^n} \rtimes H$ for p prime, where H is any subgroup of $\mathrm{Aut}(\mathbb{Z}_{p^n})$.

At the other extreme, inside $\mathrm{Hol}(G)$ is $\mathrm{InHol}(G) = \rho(G) \cdot \mathrm{Inn}(G)$, where $\mathrm{Inn}(G)$ is the group of inner automorphisms of G, automorphisms obtained by conjugation by elements of G.

Proposition 6. *If G has trivial center, then every regular embedding $\beta : \Gamma \to \mathrm{InHol}(G)$ corresponds to a fixed-point free pair of homomorphisms from Γ to G.*

This result is essentially in [CaC99].

Proof. The conjugation map $C : G \to \mathrm{Inn}(G)$, $C(\sigma)(\pi) = \sigma\pi\sigma^{-1}$ is a homomorphism with kernel equal to the center $Z(G)$ of G. If $Z(G) = (1)$, then, since $\lambda(G)$ and $\rho(G)$ centralize each other in $\mathrm{Perm}(G)$ we have isomorphisms:

$$G \times G \to \lambda(G) \cdot \rho(G) = \rho(G) \cdot \mathrm{Inn}(G)$$

by

$$(\sigma, \tau) \mapsto \lambda(\sigma) \cdot \rho(\tau) = \rho(\tau\sigma^{-1})C(\sigma)$$

with inverse

$$j : \rho(\sigma)C(\tau) = \lambda(\tau)\rho(\sigma\tau) \mapsto (\tau, \sigma\tau).$$

If $\beta : \Gamma \to \mathrm{InHol}(G)$ is a homomorphism and $Z(G) = (1)$, then the composite maps $\beta_i = \pi_i j \beta : \Gamma \to G$ (where $\pi_i, i = 1, 2$ are the projections from $G \times G$ onto the two factors) are homomorphisms from Γ to G, and $\beta(\sigma) = \lambda(\beta_1(\sigma))\rho(\beta_2(\sigma))$.

The homomorphism $\beta : \Gamma \to \mathrm{InHol}(G)$ is a regular embedding if

$$\beta(\Gamma) \cdot e = G.$$

This is the case iff

$$\{\lambda(\beta_1(\sigma))\rho(\beta_2(\sigma))(e) | \sigma \in \Gamma\} = G,$$

that is, iff

$$\{\beta_1(\sigma)\beta_2(\sigma)^{-1} | \sigma \in \Gamma\} = G,$$

iff (β_1, β_2) is a fixed-point free pair of homomorphisms from Γ to G. □

A finite group G is *complete* if G has trivial center and $\mathrm{Aut}(G) = \mathrm{Inn}(G)$. The best known examples of finite complete groups are holomorphs of non-abelian simple groups, the symmetric groups S_n for $n \geq 3, n \neq 6$, and $\mathrm{Hol}(\mathbb{Z}_p)$ for p an odd prime. The last proposition implies immediately:

Corollary 7. *If G is a finite complete group, then for every group Γ of the same cardinality as G, every regular embedding from Γ to G arises from a fixed-point free pair of homomorphisms from Γ to G.*

4. Groups of order $p(p-1)$, p a safeprime

To explore the value of fixed-point free pairs for determining Hopf–Galois structures, in this section we work through an extended example.

In [Ch03], we let p be a prime so that $p-1 = 2q$ where q is prime (then q is a Sophie Germain prime and p is a safeprime) and determined the number of equivalence classes of regular embeddings from $\Gamma = \mathrm{Hol}(\mathbb{Z}_p) = \mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$ to $\mathrm{Hol}(G)$ for each of the six isomorphism types of groups of order $p(p-1)$. It turned out that for each G there exist up to equivalence at least p regular embeddings from Γ to $\mathrm{Hol}(G)$. Subsequently, Tim Kohl [Ko11] computed the number of equivalence classes of regular embeddings from Γ to $\mathrm{Hol}(G)$ for Γ and G running through each of the six isomorphism types of groups of order $p(p-1)$. In this section we determine in each case how many of those equivalence classes arise from fixed-point free pairs of homomorphisms from Γ to G.

The six isomorphism types of groups of order $2pq$ are $\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$, D_{pq}, $(\mathbb{Z}_p \rtimes \mathbb{Z}_q) \times \mathbb{Z}_2$, $D_p \times \mathbb{Z}_q$, $D_q \times \mathbb{Z}_p$ and $\mathbb{Z}_{2pq}$, where D_n is the dihedral group of order $2n$ and $\mathbb{Z}_n$ is the cyclic group of order n (or the additive group of $\mathbb{Z}/n\mathbb{Z}$) . The first two have trivial centers. We set $F = \mathbb{Z}_p \rtimes \mathbb{Z}_q$.

Let $E(\Gamma, G)$, resp. $E_f(\Gamma, G)$, be the set of equivalence classes of regular embeddings of Γ into $\mathrm{Hol}(G)$, resp. those equivalence classes arising from fixed-point free pairs of homomorphisms from Γ to G. Let $e(\Gamma, G)$, resp. $e_f(\Gamma, G)$ be the cardinalities of $E(\Gamma, G)$, resp. $E_f(\Gamma, G)$. As noted in the introduction, elements of $E(\Gamma, G)$ are in one to one correspondence with Hopf–Galois structures on a field extension $L|K$ with Galois group Γ, where the K-Hopf algebra H acting on L has type G.

Kohl's results for $E(\Gamma, G)$ is shown in Table 1.

In this section we show:

Proposition 8. *For groups of order $p(p-1)$ with p and $q = (p-1)/2$ prime, $e_f(\Gamma, G)$ is given by Table 2.*

Note that the $\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$ columns of Table 1 and Table 2 are equal by Corollary 7.

4.1. Cases where $e_f(\Gamma, G) = 0$. We have that $e_f(\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times, G) = 0$ for $G \ncong \mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$ by Proposition 5. Also, $e_f(\Gamma, \mathbb{Z}_{2pq}) = 0$ for $G \ncong \mathbb{Z}_{2pq}$ by Proposition 4.

$\Gamma\backslash G$	$\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$	D_{pq}	$F \times \mathbb{Z}_2$	$D_p \times \mathbb{Z}_q$	$D_q \times \mathbb{Z}_p$	$\mathbb{Z}_{2pq}$
$\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$	$2(p(q-2)+1)$	$4p$	$2p(q-1)$	$2p$	$2p$	p
D_{pq}	0	4	0	$2q$	$2p$	pq
$F \times \mathbb{Z}_2$	$2p(q-1)$	$4p$	$2(p(q-2)+1)$	$2p$	$2p$	p
$D_p \times \mathbb{Z}_q$	$2p(q-1)$	4	$2p(q-1)$	2	$2p$	p
$D_q \times \mathbb{Z}_p$	0	4	0	$2q$	2	q
$\mathbb{Z}_{2pq}$	$2(q-1)$	4	$2(q-1)$	2	2	1

TABLE 1. $e(\Gamma, G)$

$\Gamma\backslash G$	$\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$	D_{pq}	$F \times \mathbb{Z}_2$	$D_p \times \mathbb{Z}_q$	$D_q \times \mathbb{Z}_p$	$\mathbb{Z}_{2pq}$
$\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$	$2(p(q-2)+1)$	0	0	0	0	0
D_{pq}	0	2	0	0	0	0
$F \times \mathbb{Z}_2$	$2p(q-1)$	0	$2(p(q-2)+1)$	0	0	0
$D_p \times \mathbb{Z}_q$	$2p(q-1)$	2	0	2	0	0
$D_q \times \mathbb{Z}_p$	0	2	0	0	2	0
$\mathbb{Z}_{2pq}$	$2(q-1)$	2	$2(q-1)$	2	2	1

TABLE 2. $e_f(\Gamma, G)$

To find the remaining cases where $e_f(\Gamma, G) = 0$, the following result is convenient.

Proposition 9. *Suppose Γ has a subgroup $\mathbb{Z}_h \rtimes \mathbb{Z}_k$ where h, k are primes and $\mathbb{Z}_k \subseteq \mathrm{Aut}(\mathbb{Z}_h)$. If all elements of order h commute with all elements of order k in G, then $\mathbb{Z}_h$ is contained in the kernel of every homomorphism from Γ to G. Hence every pair of homomorphisms from Γ to G has a nonzero fixed-point.*

Proof. Write elements of $\mathbb{Z}_h \rtimes \mathbb{Z}_k$ as (a, b^r) where a is an integer modulo h, $\mathbb{Z}_k = \langle b \rangle$ with b an integer of order k modulo h, and r is an integer modulo k, and the group multiplication is

$$(a, b^r)(c, b^s) = (a + b^r c, b^{r+s}).$$

Then in particular,

$$(0, b)(a, 1) = (ba, b) = (ba, 1)(0, b).$$

Let f be a homomorphism from Γ to G. Then

$$f(0, b)f(a, 1) = f(ba, 1)f(0, b).$$

Since $f(0, b)$ has order k or 1 in G, and $f(a, 1)$ has order h or 1, we have

$$f(0, b)f(a, 1) = f(a, 1)f(0, b),$$

so

$$f(ba, 1) = f(a, 1),$$

hence

$$f((b-1)a, 1) = 0.$$

So $(b-1)\mathbb{Z}_h$ is in the kernel of f. But since $b-1 \neq 0$, $(b-1)\mathbb{Z}_h = \mathbb{Z}_h$. Hence for every pair (f, g) of homomorphisms from Γ to G, the elements of $\mathbb{Z}_h$ are fixed-points of (f, g). □

We apply Proposition 9 to various Γ and G:

- $\Gamma = D_{pq}$. If $G = D_p \times \mathbb{Z}_q$ or $\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$, then since elements of orders 2 and q commute in G, every homomorphism from Γ to G has kernel containing $\mathbb{Z}_q \subset D_{pq}$. So $e(\Gamma, G) = 0$.

  If $G = D_q \times \mathbb{Z}_p$ or $F \times \mathbb{Z}_2$ or $\mathbb{Z}_{2pq}$, then elements of orders 2 and p commute in G, so every homomorphism from Γ to G has kernel containing $\mathbb{Z}_p \subset D_{pq}$. So $e_f(\Gamma, G) = 0$.
- $\Gamma = F \times \mathbb{Z}_2$. Since elements of order p and order q commute in $G = D_{pq}, D_p \times \mathbb{Z}_q, D_q \times \mathbb{Z}_p$ and $\mathbb{Z}_{2pq}$, Proposition 9 implies that $e(\Gamma, G) = 0$ for those G.
- $\Gamma = D_p \times \mathbb{Z}_q$. Since elements of order 2 and order p commute in $G = D_q \times \mathbb{Z}_p, (\mathbb{Z}_p \rtimes \mathbb{Z}_q) \times \mathbb{Z}_2$ and $\mathbb{Z}_{2pq}$, Proposition 9 implies that $e(\Gamma, G) = 0$ for those G.
- $\Gamma = D_q \times \mathbb{Z}_p$. Since elements of order 2 and order q commute in $G = \mathbb{Z}_p \rtimes \mathbb{Z}_p^\times, D_p \times \mathbb{Z}_q, (\mathbb{Z}_p \rtimes \mathbb{Z}_q) \times \mathbb{Z}_2$ and $\mathbb{Z}_{2pq}$, Proposition 9 implies that $e(\Gamma, G) = 0$ for those G.

We're left with computing $e_f(\Gamma, G)$ for the following cases:

- $e_f(D_p \times \mathbb{Z}_q, D_{pq})$,
- $e_f(D_q \times \mathbb{Z}_q, D_{pq})$,
- $e_f(\mathbb{Z}_{2pq}, G)$ for all five nonabelian G, and
- $e_f(\Gamma, G)$ with $\Gamma = G$ for all six Γ.

We omit the cases where $G = \mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$ since then $e_f(\Gamma, G) = e(\Gamma, G)$ by Corollary 7.

4.2. The cases where $e_f(\Gamma, G) \neq 0$, $\Gamma \ncong \mathbb{Z}_{2pq}$ and $\Gamma \ncong G$.

Proposition 10. *$e_f(D_p \times \mathbb{Z}_q, D_{pq}) = 2$.*

Proof. View $D_p \times \mathbb{Z}_q = (\mathbb{Z}_p \rtimes \mathbb{Z}_2) \times \mathbb{Z}_q$ and $D_{pq} = \mathbb{Z}_{pq} \rtimes \mathbb{Z}_2$ with $\mathbb{Z}_2$ multiplicative and the other factors additive. Every homomorphism

$$h : D_p \times \mathbb{Z}_q \to D_{pq}$$

must have the form

$$h(1, 1, 0) = (qa, 1)$$
$$h(0, -1, 0) = (d, (-1)^s)$$
$$h(0, 1, 1) = (pc, 1)$$

for some a modulo p, c modulo q, d modulo pq and s modulo 2. Since $(0, 1, 1)$ and $(0, -1, 0)$ commute, we must have

$$(d, (-1)^s)(pc, 1) = (pc, 1)(d, (-1)^s).$$

If $s = 1$, then this yields

$$-pc \equiv pc \pmod{pq},$$

hence h vanishes on $\mathbb{Z}_q$. If $s = 0$, then $d = 0$, hence applying h to the relation $(0,-1,0)(1,1,0) = (-1,1,0)(0,-1,0)$ yields $a = 0$, so h vanishes on D_p. Thus we have two types of homomorphisms from $D_p \times \mathbb{Z}_q$ to D_{pq}, namely,

$$f(1,1,0) = (qa, 1)$$
$$f(0,-1,0) = (d, -1)$$
$$f(\mathbb{Z}_q) = 0$$

and

$$g(D_p) = 0$$
$$g(0,1,1) = (pc, 1).$$

Clearly pairs consisting of two homomorphisms of type f, or two of type g cannot be fixed-point free. If qa or pc is zero modulo pq then (f, g) is not fixed-point free. Otherwise (f, g) is fixed-point free. For if

$$f(x, y, z) = g(x, y, z)$$

then

$$(qax, 1)(d, -1)^y = (pcz, 1),$$

so $y = 0$ and $qax = pcz \pmod{pq}$, and the latter holds only when p divides x and q divides z.

Since D_{pq} has trivial center, two pairs (f, g) and (f', g') are equivalent if and only if there exists an automorphism δ of D_{pq} such that $(f', g') = (\delta f, \delta g)$. Now δ is uniquely determined by

$$\delta(1,1) = (x, 1), \delta(0,-1) = (y, -1)$$

where x is coprime to pq and y is arbitrary modulo pq. Then

$$\delta f(1,1,0) = \delta(qa, 1) = (qax, 1)$$
$$\delta f(0,-1,0) = \delta(d, -1) = (dx + y, -1)$$
$$\delta g(0,1,1) = \delta(pc, 1) = (pcx, 1).$$

So if (f, g) corresponds to the parameters (qa, pc, d) with a coprime to p, c coprime to q and d arbitrary modulo pq, then $(\delta f, \delta g)$ corresponds to the parameters $(qax, pcx, dx + y)$ where x is coprime to pq and y is arbitrary modulo pq. Given (qa', pc', d') with a' coprime to p, c' coprime to q and d' arbitrary modulo pq, we seek x, y with x coprime to pq and y arbitrary so that

$$qax \equiv qa' \pmod{pq}$$
$$pcx \equiv pc' \pmod{pq}$$
$$dx + y \equiv d' \pmod{pq}.$$

These reduce to

$$ax \equiv a' \pmod{p}$$
$$cx \equiv c' \pmod{q}$$
$$dx + y \equiv d' \pmod{pq}$$

which have a unique solution $(x \mod pq, y \mod pq)$. Thus every fixed-point free pair (f, g) with $f(\mathbb{Z}_q) = 0$ and $g(D_p) = 0$ is equivalent to every other such pair. Hence, up to equivalence there are exactly two elements of $E_f(\Gamma, G)$, represented by a pair (f, g) and the transposed pair (g, f). □

Proposition 11. *$e_f(D_q \times \mathbb{Z}_p, D_{pq}) = 2$.*

By the symmetry of p and q in D_{pq} this result is identical to the last one.

4.3. The cases where $\Gamma = G$.

4.3.1. $G = \Gamma = D_q \times \mathbb{Z}_p$ or $D_p \times \mathbb{Z}_q$ or $F \times \mathbb{Z}_2$. We show:

Proposition 12. *$e_f(D_q \times \mathbb{Z}_p, D_q \times \mathbb{Z}_p) = e_f(D_p \times \mathbb{Z}_q, D_p \times \mathbb{Z}_q) = 2$, and $e_f(F \times \mathbb{Z}_2, F \times \mathbb{Z}_2) = 2(p(q-2)+1)$.*

Proof. Each such G has the form $G = (\mathbb{Z}_h \rtimes \mathbb{Z}_k) \times \mathbb{Z}_l$, where h, k, l are primes. Any endomorphism of G restricts on $\mathbb{Z}_l$ to either 0 or an automorphism of $\mathbb{Z}_l$, and restricted on $\mathbb{Z}_h \rtimes \mathbb{Z}_k$ is either an automorphism of $\mathbb{Z}_h \rtimes \mathbb{Z}_k$ or vanishes on $\mathbb{Z}_h$. We obviously cannot have a fpf pair (f, g) where both f and g vanish on $\mathbb{Z}_h$. So assume that f is an automorphism on $\mathbb{Z}_h \rtimes \mathbb{Z}_k$. If f is surjective on $\mathbb{Z}_l$, then f is an automorphism of G. On the other hand, if $f = 0$ on $\mathbb{Z}_l$, then g must restrict to a surjective map ζ on $\mathbb{Z}_l$. Extend ζ to a homomorphism on G trivial on $(\mathbb{Z}_h \times \mathbb{Z}_k)$. If (f, g) is then a fixed-point free pair, then the pair $(f', g') = (f \cdot \zeta^{-1}, g \cdot \zeta^{-1})$ is fixed-point free and f' is an automorphism of G. We conclude that every fpf pair (f, g) on G is equivalent to a pair in which one of the homomorphisms is an automorphism.

Letting δ be the inverse of that automorphism, we obtain the equivalent pair $(\delta f, \delta g)$ in which one of the maps is the identity on G. Then the other must be a fpf endomorphism of G.

Thus in all three cases, we need to find the fixed-point free endomorphisms of G. Each fixed-point free endomorphism of G restricts to a fixed-point free endomorphism of each direct summand.

There are no fixed-point free automorphisms of $\mathbb{Z}_h \rtimes \mathbb{Z}_k$ by [CCo07], Corollary 5.3. Hence, for D_p, resp. D_q, if f is a nonzero fpf endomorphism, then f must vanish on $\mathbb{Z}_p$, resp. $\mathbb{Z}_q$, so $f(1,1) = (0,1), f(0,-1) = (d,-1)$ for some d. But then $f(d,-1) = (d,-1)$, hence f has a fixed-point. Thus the only fixed-point free pairs on $\mathbb{Z}_p \times D_q$ or $\mathbb{Z}_q \times D_p$ are $(\text{identity}, 0)$ and $(0, \text{identity})$.

For $G = F \times \mathbb{Z}_2$, if $(f, \text{identity})$ is a fpf pair, then f must be zero on $\mathbb{Z}_2$ (or else $(1, (0,1))$ is a nonzero fixed-point). So we need to find the fixed-point free endomorphisms of F. That is given in [CCo07], Theorem 6.5: the number is $p(q-2)+1$. Each pair $(\text{identity}, f)$ and $(f, \text{identity})$ where f is

zero on $\mathbb{Z}_2$ and restricts to a fixed-point free endomorphism of F, gives a different equivalence class of regular embeddings of G into $\mathrm{Hol}(G)$. □

4.3.2. $G = \Gamma = D_{pq}$. We show:

Proposition 13. *$e_f(D_{pq}, D_{pq}) = 2$.*

Proof. Write elements of G as (d, e) where d is in $\mathbb{Z}_{pq}$ and $e = 1$ or -1. Any endomorphism $f : G \to G$ must satisfy one of the following:

- f is an automorphism of G (call it f_1).
- f has kernel $\mathbb{Z}_p$: call it f_p. Then $f_p(1,1) = (qs, 1), f_p(0,-1) = (b, -1)$ for some s coprime to p and some b.
- f has kernel $\mathbb{Z}_q$: call it f_q. Then $f_q(1,1) = (pr, 1), f_p(0,-1) = (c, -1)$ for some r coprime to q and some c.
- f has kernel $\mathbb{Z}_{pq}$: call it f_{pq}. Then $f_{pq}(1,1) = (0,1), f_{pq}(0,1) = (d, -1)$ for some d.
- f is trivial: call it 0.

We see if a pair (f_p, f_q) can be fixed-point free. So we try to solve

$$f_p(y,-1) = f_q(y,-1) :$$
$$(qsy, 1)(b,-1) = (pry, 1)(c,-1).$$

This holds iff

$$qsy + b \equiv pry + c;$$
$$(qs - pr)y \equiv c - b \pmod{pq}.$$

Since r is coprime to q and s is coprime to p, $qs - pr$ is coprime to p and coprime to q, hence is a unit modulo pq. Thus there is a unique y solving $f_p(y,-1) = f_q(y,-1)$. Hence (f_p, f_q) cannot be fixed-point free.

Thus if (f, g) is a fixed-point free pair on D_{pq}, then f or g must be an automorphism. Up to equivalence by automorphisms, then, we may assume that every fixed-point free pair has the form $(f, \mathrm{identity})$ or $(\mathrm{identity}, f)$, where f is a fixed-point free endomorphism of G.

Lemma 14. *Every nonzero endomorphism of D_{pq} has a fixed-point.*

Proof. Let $f(1,1) = (m, 1), f(0,-1) = (b, -1)$. If $m = 1$ then $(1,1)$ is a fixed-point; if $m = 1 + pr$, then $(q, 1)$ is a fixed-point; if $m = 1 + qs$ then $(p, 1)$ is a fixed-point. If m is not congruent to 1 modulo p or modulo q, then $1 - m$ is a unit modulo pq, and then we may find a fixed-point of the form $(y, -1)$:

$$f(y,-1) = (ym, 1)(b,-1) = (ym + b, -1).$$

Solving $y = ym + b$ is the same as solving $(1 - m)y = b$ for y; since $1 - m$ is a unit modulo pq, this has a unique solution for y. □

So up to equivalence, the only fpf pairs are $(\mathrm{identity}, 0)$ and $(0, \mathrm{identity})$. That completes the proof of Proposition 13. □

4.4. The cases where $\Gamma = \mathbb{Z}_{2pq}$. There are common features in the determination of $e_f(\mathbb{Z}_{2pq}, G)$ for all G.

Proposition 15. *Let $\Gamma = \mathbb{Z}_{rs}$ (written additively) with $(r,s) = 1$, let G be a group of order rs and suppose G has an element a of order r and an element b of order s. Let $f_r, f_s : \Gamma \to G$ be defined by $f_r(1) = a, f_s(1) = b$. Then (f_r, f_s) is a fpf pair.*

Proof. It suffices to show that $f_r(x) = f_s(x)$ only for $x = 1$. But $f_r(x) = a^x$ has order dividing r and $f_s(x) = b^x$ has order dividing s. Since $(r,s) = 1$, $a^x = b^x = 1$ in $\mathbb{Z}_{rs}$. So both r and s divide x. □

In what follows, f_r will denote some homomorphism from $\mathbb{Z}_{rs}$ to G so that $f_r(1)$ has order r.

For groups of order $2pq$, Proposition 15 shows that we have fpf pairs f_r, f_s for every factorization $2pq = rs$ where G has elements of order r and s. So we look for maximal numbers in the lattice of orders of elements of G:

G	$\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$	D_{pq}	$F \times \mathbb{Z}_2$	$D_p \times \mathbb{Z}_q$	$D_q \times \mathbb{Z}_p$
maximal orders	$p, 2q$	$pq, 2$	$2p, 2q$	$pq, 2q$	$pq, 2p$
order of center	1	1	2	q	p
possible fpf pairs	(f_p, f_{2q}) (f_{2q}, f_p)	(f_{pq}, f_2) (f_2, f_{pq})	(f_{2p}, f_q) (f_q, f_{2p}) (f_p, f_{2q}) (f_{2q}, f_p)	(f_{pq}, f_2) (f_2, f_{pq}) (f_p, f_{2q}) (f_{2q}, f_p)	(f_{pq}, f_2) (f_2, f_{pq}) (f_q, f_{2p}) (f_{2p}, f_q)

We need to consider the equivalence relation on fpf pairs. Recall that two pairs (f,g) and (f',g') are equivalent iff

$$f' = \delta f \cdot \zeta, \quad g' = \delta g \cdot \zeta$$

for some automorphism δ of G and some homomorphism $\zeta : \Gamma \to Z(G)$.

First we look at the action on pairs by multiplication by homomorphisms from Γ to the center of G.

Proposition 16. *Suppose Γ is cyclic of order $n = rsz$, distinct primes, and G has order n with the center $Z(G)$ of G of order z. Then every fixed-point free pair (f,g) with $f, g : \Gamma \to G$ is equivalent to a pair of form (f_r, f_{sz}) or of form (f_s, f_{rz}).*

Proof. View $\Gamma = \mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle$. Suppose (f,g) is a fpf pair. Then the least common multiple of the orders of $f(1)$ and $g(1)$ must be n. Also, since the center of G has order z, elements of order r and of order s in G cannot commute, so rs cannot divide the order of $f(1)$ or the order of $g(1)$.

Thus if $f(1)$ has order r, then $g(1)$ must have order sz and (f,g) has the form (f_r, f_{sz}). So suppose $f(1) = a$, an element of order $m = rz$ in G. We find $\zeta : \Gamma \to Z(G)$ so that $f(1) \cdot \zeta(1)$ has order r. Let $a^r = c$, then c has order z, so is in $Z(G)$. Since $(r,z) = 1$, $c = d^r$ for some d in $Z(G)$. Define $\zeta : \Gamma \to Z(G)$ by $\zeta(1) = d^{-1}$. Then $f(r)\zeta(r) = 1$, so $f(1) \cdot \zeta(1)$ has order

r. Then $g(1)\cdot\zeta(1)$ must have order sz, and thus $(f\cdot\zeta, g\cdot\zeta)$ has the form (f_r, f_{sz}). □

We observe that for any automorphism δ of G and any homomorphism $\zeta : \Gamma \to Z(G)$, if $f(1)$ has order r, then $\delta(f(1)\zeta(1))$ cannot have order divisible by s. Applying this observation and Proposition 16 to groups G of order $2pq$ yields the following table of representatives of fixed-point free pairs under equivalence by multiplication by maps $\zeta : \Gamma \to G$:

G	$\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$	D_{pq}	$F \times \mathbb{Z}_2$	$D_p \times \mathbb{Z}_q$	$D_q \times \mathbb{Z}_p$
maximal orders	$p, 2q$	$pq, 2$	$2p, 2q$	$pq, 2q$	$pq, 2p$
order of center	1	1	2	q	p
possible fpf pairs	(f_p, f_{2q}) (f_{2q}, f_p)	(f_{pq}, f_2) (f_2, f_{pq})	(f_p, f_{2q}) (f_q, f_{2p})	(f_p, f_{2q}) (f_2, f_{pq})	(f_2, f_{pq}) (f_q, f_{2p})

To determine the number of orbits of pairs under equivalence, every orbit has a pair (f, g) of the form (f_h, f_k) for $|\Gamma| = hk = 2pq$, and any automorphism δ of G maps a pair of the form (f_h, f_k) to another pair of the same form. So we need to look at the number of orbits of pairs (f_h, f_k) under the action of $\mathrm{Aut}(G)$. But since $f_h(1)$ has order h and $f_k(1)$ has order k where h and k are coprime, and automorphisms of G act on the set of elements of order h and on the set of elements of order k, we can look at the orbits of $\mathrm{Aut}(G)$ on each of these sets.

For $G = D_{pq}, D_p \times \mathbb{Z}_q$ and $D_q \times \mathbb{Z}_p$, it is routine to check that given any two pairs of elements $(a, b), (a', b')$ of orders (h, k) as in the last table, then there exists an automorphism of G taking one to the other. Thus all pairs (f_h, f_k) for the same h, k are equivalent. Hence for those G,

$$e_f(\Gamma, G) = 2.$$

For $G = F \times \mathbb{Z}_2$, an automorphism of G fixes the $\mathbb{Z}_2$ component and acts as an automorphism of $F = \mathbb{Z}_p \rtimes \mathbb{Z}_q$. For $G = \mathbb{Z}_p \rtimes \mathbb{Z}_{2q}$ or for F, an automorphism δ is defined by

$$\delta(1, 1) = (x, 1), \delta(0, b) = (y, b).$$

(To see this, suppose $\delta(0, b) = (y, b^t)$. Then since $(0, b)(1, 1) = (b, b) = (b, 1)(0, b)$, applying δ yields $(y, b^t)(x, 1) = (bx, 1)(y, b^t)$, hence $y + b^t x = bx + y$. Thus $(b^t - b)x = 0$. But since δ is an automorphism, $x \neq 0$, so $b^t = b$.) It follows that for $G = F \times \mathbb{Z}_2$, $\mathrm{Aut}(G)$ partitions $\{(f_{2p}, f_q)\}$ into $q - 1$ orbits, one for each element b of order q in F. Hence

$$e_f(\Gamma, F \times \mathbb{Z}_2) = 2(q - 1).$$

For $G = \mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$, $\mathrm{Aut}(G)$ partitions $\{(f_p, f_{2q})\}$ into $\phi(2q) = q - 1$ orbits. So

$$e_f(\Gamma, \mathbb{Z}_p \rtimes \mathbb{Z}_{2q}) = 2(q - 1).$$

That completes the entries of Table 2.

Remark 17. Let $\Gamma = \mathbb{Z}_{pq} = \mathbb{Z}_p \times \mathbb{Z}_q$ where p, q are primes with $p \equiv 1 \pmod{q}$. [By04] showed that there are $2q-1$ Hopf–Galois structures on a Galois extension of fields with Galois group Γ. One of them is the classical structure by the Galois group Γ.

Above, we did the case where $\Gamma = \mathbb{Z}_{2pq} = \mathbb{Z}_2 \times \mathbb{Z}_p \times \mathbb{Z}_q$ where q is prime and divides $p-1$, and $G = \mathbb{Z}_2 \times F$ where $F = \mathbb{Z}_p \rtimes \mathbb{Z}_q$. If (f_{2p}, f_q) is a fpf pair, then (since $f_{2p}(1)$ has order $2p$), f_{2p} restricts to the identity on $\mathbb{Z}_2$, hence (f_{2p}, f_q) restricts to a fpf pair (f_p, f_q) from $\mathbb{Z}_p \times \mathbb{Z}_q$ to $\mathbb{Z}_p \rtimes \mathbb{Z}_q$. Conversely, every such pair (f_p, f_q) extends to a pair (f_{2p}, f_q) from $\mathbb{Z}_{2pq}$ to $\mathbb{Z}_2 \times F$ by letting f_{2p} be the identity on $\mathbb{Z}_2$. The equivalence by automorphisms δ on F is the same as on $\mathbb{Z}_2 \times F$ since every automorphism of $F \times \mathbb{Z}_2$ is the identity on $\mathbb{Z}_2$. Thus the computation in the last case above shows that $e_f(\mathbb{Z}_{pq}, F) = 2(q-1)$.

The computation of [By04] implies that $2(q-1) \geq e(\mathbb{Z}_{pq}, F)$. Thus

$$2(q-1) = e_f(\mathbb{Z}_{pq}, F) = e(\mathbb{Z}_{pq}, F)$$

and we conclude:

Proposition 18. *Let $L|K$ be a Galois extension with Galois group $\Gamma = \mathbb{Z}_{pq}$ where p, q are primes with q dividing $p-1$. Then every nonclassical Hopf–Galois structure on $L|K$ corresponds to a fixed-point free pair of homomorphisms from Γ to F.*

5. Nonabelian Hopf–Galois structures

Here is a simple application of the idea behind the computations of $e_f(\Gamma, G)$ where $\Gamma = \mathbb{Z}_{2pq}$, above.

Proposition 19. *Let $G = H_1 \rtimes H_2$ be a semidirect product of two finite groups H_1 and H_2. Let $\Gamma = H_1 \times H_2$. Then there exists a regular embedding β of Γ into $\mathrm{Hol}(G)$. Hence if $L|K$ is a Galois extension with Galois group Γ, there exists a Hopf–Galois structure on $L|K$ where the K-Hopf algebra has type G.*

Proof. Let $\pi_i : \Gamma \to H_i$ be the projection map, and $j_i : H_i \to G$ the inclusion. Then $(f_1, f_2) = (j_1\pi_1, j_2\pi_2)$ is a fixed-point free pair of homomorphisms from Γ to G, hence yields a regular embedding of Γ into $\mathrm{Hol}(G)$. By [By96] such a regular embedding yields a Hopf–Galois structure on $L|K$ of type G. □

This has the following interesting consequence:

Theorem 20. *Let p be prime. Let $L|K$ be a Galois extension of fields with Galois group Γ, a noncyclic abelian p-group of order p^n, $n \geq 3$. Then $L|K$ admits a nonabelian Hopf–Galois structure.*

Proof. Let $\Gamma = \mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times \ldots \times \mathbb{Z}_{p^{n_k}}$ where $1 \leq n_1 \leq \ldots \leq n_k$. By Proposition 19 it suffices to find a nontrivial semidirect product $G = H \rtimes_\alpha K$

where $H \cong \mathbb{Z}_{p^{n_2}} \times \ldots \times \mathbb{Z}_{p^{n_k}}$, $K \cong \mathbb{Z}_{p^{n_1}}$, and $\alpha : K \to \mathrm{Aut}(H)$ is a nontrivial homomorphism.

If Γ is elementary abelian, then $H = \mathbb{F}_p^{n-1}$ and $n-1 \geq 2$. So $GL_{n-1}(\mathbb{F}_p)$ has an element A of order p, as the order of $GL_{n-1}(\mathbb{F}_p)$ is

$$(p^{n-1}-1)(p^{n-1}-p)\cdots(p^{n-1}-p^{n-2}).$$

Let $\alpha : K \to GL_{n-1}(\mathbb{F}_p) = \mathrm{Aut}(H)$ by $\alpha(1) = A$. Then $G = H \rtimes_\alpha K$ is a nontrivial semidirect product.

If $n_k \geq 2$, let $H = \mathbb{Z}_{p^{n_2}} \times \cdots \times \mathbb{Z}_{p^{n_k}}$, and let b in $\mathbb{Z}$ be coprime to p and have order p modulo p^{n_k}. Let $K = \mathbb{Z}_{p^{n_1}}$ and let $\alpha : K \to \mathrm{Aut}(H)$ by $\alpha(1) =$ diagonal multiplication by b:

$$\alpha(1)(a_2, \ldots a_{n_k}) = (ba_2, \ldots, ba_{n_k}).$$

Then $G = H \rtimes_\alpha K$ is a nontrivial semidirect product. □

To set Theorem 20 in context, let $L|K$ be a Galois extension of fields with Galois group Γ. For p an odd prime, Kohl [Ko98] proved that if Γ is a cyclic p-group, then Γ is the type of every K-Hopf algebra giving a Hopf–Galois structure on $L|K$, and [By96] showed that the same is true if $\Gamma = \mathbb{Z}_p \times \mathbb{Z}_p$. For $p = 2$, [By07] showed that for Γ cyclic of order 2^e, $e \geq 3$, then $L|K$ admits a nonabelian Hopf–Galois structure. Theorem 20 completes the determination of which $L|K$ with abelian p-group Γ admit a nonabelian Hopf–Galois structure.

If Γ is an abelian p-group of p-rank m and $p > m+1$, then by a theorem of Featherstonhaugh et al. [FCC12], every *abelian* Hopf–Galois structure on $L|K$ must have type Γ. Theorem 20 implies the impossibility of extending that theorem to all Hopf–Galois structures on $L|K$ (except in the cases covered by [Ko98] and [By96]).

For groups of even order divisible by at least two distinct primes, we have:

Proposition 21. *Let Γ be abelian of even order $2^e q$ with $q > 1$ odd. Let $L|K$ be a Galois extension of fields with Galois group Γ. Then $L|K$ admits a nonabelian Hopf–Galois structure.*

Proof. Letting K be a cyclic direct factor of Γ of order a power of 2, and H the complementary direct factor, define a homomorphism α from K to $\mathrm{Aut}(H)$ by mapping the generator of K to multiplication by -1. Then $G = H \rtimes_\alpha K$ is a nontrivial semidirect product. □

Corollary 22. *A finite abelian Galois extension of fields of even degree d admits a nonabelian Hopf–Galois structure if and only if $d > 4$.*

We are left with a finite abelian Galois extension of fields with Galois group Γ of odd order, divisible by at least two primes. Under what conditions on Γ does the extension admit a nonabelian Hopf–Galois structure?

If Γ has a p-primary direct factor P and Proposition 19 applies to yield a fpf pair of homomorphisms from P to a nonabelian semidirect product

of the same order, then it is clear that by extending the fpf pair to all of Γ by letting one of the homomorphisms be the identity and the other be 0 on the complementary direct factor to P, we obtain a fpf pair from Γ to a nonabelian semidirect product. That applies to any abelian group Γ with a p-primary component which is noncyclic of order p^n, $n \geq 3$. So the question is only of interest for groups Γ whose p-primary components are elementary abelian of p-rank 2 or cyclic. Among those groups we can characterize the ones for which Proposition 19 applies to give nonabelian Hopf–Galois structures:

Proposition 23. *Let*

$$\Gamma = \prod_{p\in\Theta} \mathbb{Z}_p^2 \times \prod_{p\in\Psi} \mathbb{Z}_{p^{e_p}},$$

where Θ and Ψ are disjoint sets of odd primes. Let $P = \Theta \cup \Psi$. There is a decomposition $\Gamma = H \times K$ with the orders of H and K coprime and a nontrivial semidirect product of the form $G = H \rtimes_\alpha K$, if and only if $(q, p-1) > 1$ for some p, q in P or $(q, p+1) > 1$ for some p in Θ and q in P.

Proof. This is similar to the proofs above. If $(q, p-1) > 1$ for some p, q in P, then let K be the q-primary component of Γ and let H be the complementary direct factor of Γ. Then H has a cyclic direct factor H_0 of order a power of p, so $\mathrm{Aut}(H_0)$ has an element b of order q, since q divides $p-1$. If K is cyclic, let $\alpha : K \to H$ map a generator of K to the automorphism that is multiplication by b on H_0 and the identity on the other direct factors of H. If $K = \mathbb{Z}_q^2$, let $\alpha : K \to H$ map a generator of a cyclic direct factor of K to the automorphism that is multiplication by b on H_0 and the identity on the other direct factors of H, and let α be trivial on a complementary direct factor of K. Then $H \rtimes_\alpha K$ is a nontrivial semidirect product. If $(q, p+1) > 1$ for some p in Θ, then let K be as before and let $H = H_0 \times H'$, where $H_0 = \mathbb{Z}_p^2$. Since $p+1$ divides the order of $GL_2(\mathbb{F}_p)$ and q divides $p+1$, there is an element A in $GL_2(\mathbb{F}_p)$ of order q. Let $\alpha : K \to \mathrm{Aut}(H)$ map the generator of a direct factor of K (if K is not cyclic), or the generator of K (if K is cyclic) to the automorphism that is multiplication by A on H_0 and the identity on H', and extend α trivially, as above, to all of K. Then $H \rtimes_\alpha K$ is a nontrivial semidirect product and the orders of H and K are coprime.

Conversely, suppose $\Gamma = H \times K$ with the orders of H and K coprime, and suppose $G = H \rtimes_\alpha K$ for some nontrivial homomorphism $\alpha : K \to \mathrm{Aut}(H)$. Then $(q, p-1) > 1$ for some p, q in P or $(q, p+1) > 1$ for some p in Θ and q in P. To see this, let K_0 be a cyclic q-group that is a direct summand of K on which α is nontrivial. Let $K = K_0 \times K'$. Then we may define a new homomorphism $\alpha_0 : K \to \mathrm{Aut}(H)$ by: α_0 is trivial on K' and is $= \alpha$ on K_0. Now $H = \prod H_p$ where the H_p are the p-primary direct summands of H, and either H_p is cyclic (hence p is in Ψ) or elementary abelian of order p^2 (hence

p is in Θ). We have $\mathrm{Aut}(H) = \prod \mathrm{Aut}(H_p)$. Since α_0 is nontrivial from K_0 to $\mathrm{Aut}(H)$, there is some p so that α_0 followed by projection onto $\mathrm{Aut}(H_p)$ is nontrivial. Thus α induces a nontrivial homomorphism from $K_0 = \mathbb{Z}/q^e\mathbb{Z}$ to either $\mathrm{Aut}(\mathbb{Z}/p^e\mathbb{Z})$ or $GL_2(\mathbb{F}_p)$. Since q and p are coprime, we must have that $(q^e, p^{e-1}(p-1)) > 1$, hence $(q, p-1) > 1$, or $(q^e, (p^2-p)(p^2-1)) > 1$, hence $(q, (p+1)(p-1)) > 1$. □

What about groups Γ of the form in Proposition 23 for which that proposition does not yield nonabelian Hopf–Galois structures?

One class of groups is handled by a 107 year old result of L. E. Dickson [Di05] (cf. [DF99], Section 5.5, Exercise 24, p. 189): every group of order n is abelian if and only if $n = p_1^{e_1}p_2^{e_2}\cdots p_n^{e_n}$ where all $e_i < 3$ and p_i does not divide $p_j^{e_j} - 1$ for all i, j. Thus if the order of Γ satisfies the assumptions of Dickson's Theorem, then there is no nonabelian Hopf–Galois structure.

This leaves as an open question the existence of nonabelian Hopf–Galois structures for Galois groups Γ of odd order whose p-primary components have order $\le p^2$, but to which Dickson's Theorem and Proposition 23 do not apply (examples: $\Gamma = \mathbb{Z}_3^2 \times \mathbb{Z}_{11^2}$ and $\Gamma = \mathbb{Z}_{3^2} \times \mathbb{Z}_{11^2}$), and groups Γ containing cyclic p-primary components of order p^e, $e \ge 3$ to which Proposition 23 does not apply (examples: $\Gamma = \mathbb{Z}_7^3 \times \mathbb{Z}_{19}$ and $\Gamma = \mathbb{Z}_{11}^3 \times \mathbb{Z}_7$).

6. New examples of abelian Γ admitting only Hopf–Galois structures of type Γ

As is illustrated in Section 4 by Table 1, from [Ko11], it is possible, and perhaps not uncommon, for a Galois group Γ to yield Hopf–Galois structures on $L|K$ of every possible type. There is a rather small list of Galois groups Γ for which it is known that every Hopf–Galois structure must have type Γ: these include cyclic p-groups with p odd [Ko98], $\mathbb{Z}_p \times \mathbb{Z}_p$ with p odd [By96], groups whose order n satisfies $(n, \varphi(n)) = 1$ (where φ is the Euler totient function) [By96], and nonabelian simple groups [By04b]. In Theorems 24 and 25 below, we will add some new classes of abelian groups to this list. These will include the four groups mentioned in the last paragraph of the preceding section. In both cases, nonabelian groups of order $|\Gamma|$ exist (as can be seen from Dickson's Theorem), but they cannot arise as the type of a Hopf–Galois structure on a Galois extension with group Γ.

We remark that if we ask for abelian groups Γ for which every *abelian* Hopf–Galois structure has type Γ, one has in addition [FCC12] for p-groups Γ of p-rank m with $p > m+1$. In [By12] it is shown that this can be extended to abelian groups Γ of order divisible by more than one prime, allowing conditions to be given under which every abelian Hopf–Galois structure has type Γ (and hence, if $|\Gamma|$ also satisfies the criterion in Dickson's Theorem, *every* Hopf–Galois structure has type Γ).

Theorem 24. *Let p, q be primes such that $2 < q < p$ and $(q, p+1) > 1$ (e.g., $q = 3$, $p = 11$), and let $\Gamma = H \times K$ where $H = \mathbb{Z}_{p^2}$ and $|K| = q^2$.*

Then every Hopf–Galois structure on a Galois extension with group Γ is of type Γ, and in particular is abelian. There are precisely pq (resp. pq^2) such Hopf–Galois structures if $K = \mathbb{Z}_{q^2}$ (resp. $K = \mathbb{Z}_q^2$).

Theorem 25. *Let Γ be a cyclic group of order $n = p^3q$, where p, q are distinct primes such that $(p, q-1) = (q, p^2-1) = 1$ but $(q, p^3-1) > 1$ (e.g., $p = 7, q = 19$ or $p = 11$, $q = 7$; note these conditions imply that p, q are odd). Then every Hopf–Galois structure on a Galois extension with group Γ is of type Γ, and in particular is abelian. There are precisely p^2 such Hopf–Galois structures.*

6.1. Groups of order p^2q^2. Let $n = p^2q^2$, where p and q are primes such that $2 < q < p$ and $(q, p+1) > 1$ as in Theorem 24. Observe that $p \geq q+2$, so $(q, p-1) = (p, q-1) = (p, q+1) = 1$. To prove Theorem 24 we need a sequence of propositions.

Proposition 26. *Let G be a nonabelian group of order n. Then $G = H' \rtimes_\alpha K'$ where $H' \cong \mathbb{Z}_p \times \mathbb{Z}_p$, K' has order q^2, and α is a nontrivial homomorphism $K' \longrightarrow \mathrm{Aut}(H')$ whose image is cyclic.*

Proof. Since $(p, q^2-1) = 1$, G has a unique (and hence normal) Sylow p-subgroup H'. The groups H' and G/H' have coprime orders p^2 and q^2, so the Schur-Zassenhaus theorem guarantees that G is a semidirect product $H' \rtimes_\alpha K'$ for some K' of order q^2 and some α. As G is nonabelian, α cannot be trivial, so $(q^2, |\mathrm{Aut}(H')|) > 1$. Since $(q, |\mathrm{Aut}(\mathbb{Z}_{p^2})|) = (q, p^2-p) = 1$, we must have $H' \cong \mathbb{Z}_p^2$. We identify $\mathrm{Aut}(H')$ with $GL_2(\mathbb{F}_p)$. If $A \neq I$ is a matrix in the image of α then A has order q or q^2 (the latter only being possible if $q^2 \mid (p+1)$ and K' is cyclic). If B is another matrix in the image of α then A and B commute, so the image of α is contained in the centralizer of the subring $\mathbb{F}_p[A]$ in the matrix ring $M_2(\mathbb{F}_p)$. But since $(q, p-1) = 1$, the characteristic polynomial of A over $\mathbb{F}_p$ cannot have a root in $\mathbb{F}_p$, so is irreducible of degree 2. Thus $\mathbb{F}_p[A]$ has $\mathbb{F}_p$-dimension 2. By the Double Centralizer Theorem (see, e.g., [Pi82], Section 12.7) the centralizer of $\mathbb{F}_p[A]$ in $M_2(\mathbb{F}_p)$ is therefore just $\mathbb{F}_p[A]$ itself, so B must lie in the cyclic group $\mathbb{F}_p[A]^\times$ of order p^2-1. Hence the image of α is cyclic. □

To work in the holomorph $\mathrm{Hol}(G)$ of the nonabelian group G in Proposition 26, we need to consider an iterated semidirect product: we have $G = H' \rtimes_\alpha K'$ and $\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G)$. For clarity of notation, we write elements of G in the form $g = [u, k]$ with $u \in H'$ and $k \in K'$, and elements of $\mathrm{Hol}(G)$ as (g, θ) with $g \in G$ and $\theta \in \mathrm{Aut}(G)$. The multiplication in G is then given by $[u, k][v, l] = [u + \alpha(k)v, kl]$, taking the operation in H' to be addition of vectors in $\mathbb{F}_p^2$.

Proposition 27. *Let $\theta \in \mathrm{Aut}(G)$ have p-power order. Then, for each $k \in K'$, there is some $w_k \in H'$ such that $\theta([u, k]) = [u + w_k, k]$ for all $u \in H'$.*

Proof. Since H' is a characteristic subgroup of G, θ must induce automorphisms of the subgroup H' and the quotient group $G/H' \cong K'$ of G. As $(p, |\operatorname{Aut}(K')|) = 1$, the automorphism on K' is trivial. Thus there exist $A \in GL_2(\mathbb{F}_p)$ of p-power order and $w_k \in H'$ for each $k \in K'$ such that $\theta([u, e_{K'}]) = [Au, e_{K'}]$ for all $u \in H'$ and $\theta([0, k]) = [w_k, k]$. Applying θ to the relation $[u, e_{K'}][0, k] = [0, k][\alpha(k)^{-1}u, e_{K'}]$, we find that $Au + w_k = w_k + \alpha(k)A\alpha(k)^{-1}u$ for all $u \in H'$ and $k \in K'$, so that A commutes with the image of α. But, as we have seen in the proof of Proposition 26, the centralizer in $GL_2(\mathbb{F}_p)$ of the image of α has order $p^2 - 1$. Since A has p-power order, this means that $A = I$. We then have $\theta([u, k]) = \theta([u, e_{K'}][0, k]) = [u, e_{K'}][w_k, k] = [u + w_k, k]$ for all $u \in H'$ and $k \in K'$. □

Proposition 28. *For G as in Proposition* 26*, there is no element of order p^2 in* $\operatorname{Hol}(G)$*.*

Proof. Let Ω be an element of $\operatorname{Hol}(G)$ of p-power order. Then $\Omega = (g, \theta)$ where $\theta \in \operatorname{Aut}(G)$ has p-power order, and $g = [u, k] \in G$ with $u \in H'$, $k \in K'$. It follows from Proposition 27 that $\theta^r([u, k]) = [u + rw_k, k]$ for all $r \in \mathbb{Z}$, so that θ^p is the identity. A simple induction shows that $\Omega^s = ([x_s, k^s], \theta^s)$ for all $s \in \mathbb{Z}$, where $x_s \in H'$ is given by

$$x_s = (1 + \alpha(k) + \cdots \alpha(k)^{s-1})u + (\alpha(k) + 2\alpha(k)^2 + \cdots + (s-1)\alpha(k)^{s-1})w_k.$$

As the order of k is a power of q, it follows that $k = e_{K'}$, and hence

$$x_p = pu + \frac{1}{2}(p-1)pw_k = 0.$$

So Ω has order at most p. □

Proof of Theorem 24. The Hopf–Galois structures here correspond to equivalence classes of regular embeddings $\beta\colon \Gamma = H \times K \longrightarrow \operatorname{Hol}(G)$ for groups G of order n.

If G is nonabelian, it must be as described in Proposition 26. By Proposition 28, the direct factor $H = \mathbb{Z}_{p^2}$ of Γ cannot embed in $\operatorname{Hol}(G)$. We can therefore assume that G is abelian, say $G = H' \times K'$ with H' of order p^2 and K' of order q^2. We claim that for a regular embedding β to exist, we must have $G \cong \Gamma$. This follows from Theorem 3 of [By12], but for completeness we give a more direct (and less general) argument here. Since H' and K' are characteristic subgroups of G, we have $\operatorname{Aut}(G) = \operatorname{Aut}(H) \times \operatorname{Aut}(K)$ and hence $\operatorname{Hol}(G) = \operatorname{Hol}(H) \times \operatorname{Hol}(K)$. The hypotheses on p and q give $(p, |\operatorname{Hol}(K')|) = 1$, so the image of H in $\operatorname{Hol}(K')$ is trivial. Thus H must embed in $\operatorname{Hol}(H')$. Moreover, since Γ is regular (and hence transitive) on G, it follows that H must be transitive (and hence regular) on H'. So we have a regular embedding $H \longrightarrow \operatorname{Hol}(H')$. Since $H = \mathbb{Z}_{p^2}$ with $p > 2$, it follows from [By96] that $H' \cong H \cong \mathbb{Z}_{p^2}$. But then $(q, |\operatorname{Aut}(H')|) = 1$, and a

similar argument gives $K' \cong K$. Thus $G \cong \Gamma$. Moreover, the regular embedding β is just the direct product of regular embeddings $\beta_1 \colon H \longrightarrow \mathrm{Hol}(H')$ and $\beta_2 \colon K \longrightarrow \mathrm{Hol}(K')$. By [By96] again, there are p equivalence classes of embeddings β_1, and q (resp. q^2) equivalence classes of β_2 for $K = \mathbb{Z}_{q^2}$ (resp. $K = \mathbb{Z}_q^2$), giving pq (resp. pq^2) equivalence classes of β. Hence the number of Hopf Galois structures is as asserted. □

We now relax the assumption on p and q. Theorem 24 allows us to settle the question of which abelian groups of order p^2q^2 yield a nonabelian Hopf–Galois structure.

Corollary 29. *Let $q < p$ be arbitrary primes, and let Γ be an abelian group of order p^2q^2. Then a Galois extension with group Γ admits a nonabelian Hopf–Galois structure if and only if either:*

(1) $(q, p-1) > 1$, *or*
(2) Γ *contains a direct factor* $\mathbb{Z}_p^2$ *and* $(q, p+1) > 1$.

Proof. If either (1) or (2) holds, then Proposition 23 gives a nontrivial semidirect product yielding a nonabelian Hopf–Galois structure. Assume now that neither (1) nor (2) holds, so that in particular $q > 2$. If $(q, p+1) > 1$ then Γ contains a direct factor $\mathbb{Z}_{p^2}$, and every Hopf–Galois structure is abelian by Theorem 24. If $(q, p+1) = 1$ then $(q, p^2-1) = 1$ and, since $p > q+1$, also $(p, q^2-1) = 1$. Then every group of order p^2q^2 is abelian by Dickson's Theorem. □

6.2. Groups of order p^3q. To prove Theorem 25, we again give some preliminary propositions.

Proposition 30. *Let H be a group of order p^3 and let θ be an automorphism of H of order $r > 1$ with $(r, p(p^2-1)) = 1$. Then H is isomorphic to $\mathbb{Z}_p^3$, and there is no subgroup of H of order p or p^2 which is invariant under θ.*

Proof. We claim that there is no normal subgroup J of H of order p or p^2 which is invariant under θ and contained in the center $Z(H)$ of H. This will suffice since if H is nonabelian we can take $J = Z(H)$ (of order p), and if J is abelian but not of exponent p we can take J to be the maximal exponent p subgroup.

Suppose such a subgroup J exists. Then θ induces automorphisms on J and H/J. Each of these groups has order p or p^2, so the condition on r forces the induced automorphisms to be the identity. Thus $\theta(h) = h\phi(h)$ for all $h \in H$, where ϕ is a function from H to $J \leq Z(H)$ which takes J to e_H. It is easily verified that ϕ is a homomorphism and that $\theta^m(h) = h\phi(h)^m$ for all $m \in \mathbb{Z}$. Hence θ^{p^2} is the identity. This is impossible since $(r, p) = 1$ and $r > 1$. □

Now let $n = p^3q$ where p, q are as in Theorem 25.

Proposition 31. *Any group of order n either has the form $H \times \mathbb{Z}_q$ where H is one of the five groups of order p^3, or has the form $\mathbb{Z}_p^3 \rtimes \mathbb{Z}_q$, where the generator of $\mathbb{Z}_q$ acts as a matrix $A \in GL_3(\mathbb{F}_p)$ of order q whose minimal polynomial over $\mathbb{F}_p$ is irreducible of degree 3.*

Proof. Any group G of order n has a normal Sylow p-subgroup H of order p^3. A Sylow q-subgroup acts on this by conjugation inside G. If this action is trivial then $G = H \times \mathbb{Z}_q$ for some H of order p^3. If the action is nontrivial, we have $H = \mathbb{Z}_p^3$ by Proposition 30, so that G is the semidirect product $(\mathbb{F}_p)^3 \rtimes \langle A \rangle$ for some matrix A of order q in $GL_3(\mathbb{F}_p)$.

By Proposition 30, A does not have an invariant subspace of $\mathbb{F}_p^3$ of dimension 1 or 2. So the minimal polynomial of A can have no irreducible factors of degree 1 or 2 over $\mathbb{F}_p$. It is therefore irreducible of degree 3. □

Proposition 32. *For a nonabelian group $G = \mathbb{Z}_p^3 \rtimes \mathbb{Z}_q$ as in Proposition 31, every element of $\mathrm{Aut}(G)$ of p-power order is conjugation by an element of $\mathbb{Z}_p^3$, and therefore has order 1 or p.*

Proof. Write the elements of G as $(\mathbf{v}, A^r)$ where $\mathbf{v} \in \mathbb{F}_p^3$ and A is a fixed element of $GL_3(\mathbb{F}_p)$ of order q. Then the multiplication in G is

$$(\mathbf{v}, A^r)(\mathbf{w}, A^s) = (\mathbf{v} + A^r\mathbf{w}, A^{r+s}).$$

Let $\theta \in \mathrm{Aut}(G)$ have p-power order. Then θ induces automorphisms of p-power order on the characteristic subgroup $\mathbb{Z}_p^3$ and the quotient $\mathbb{Z}_q$, the latter induced automorphism being the identity since $(p, q-1) = 1$. Thus $\theta(\mathbf{v}, I) = (C\mathbf{v}, I)$ for all $\mathbf{v}$, where $C \in GL_3(\mathbb{F}_p)$ has p-power order, and $\theta(0, A) = (\mathbf{d}, A)$ for some $\mathbf{d} \in \mathbb{F}_p^3$. The relation $(0, A)(\mathbf{v}, I) = (A\mathbf{v}, I)(0, A)$ gives $(\mathbf{d} + AC\mathbf{v}, A) = (CA\mathbf{v} + \mathbf{d}, A)$, so that C commutes with A. But by Proposition 31, the subring $\mathbb{F}_p[A] \cong \mathbb{F}_{p^3}$ in the matrix ring $M_3(\mathbb{F}_p)$ has $\mathbb{F}_p$-dimension 3. Using the Double Centralizer Theorem as in the proof of Proposition 26, we find that C must lie in $\mathbb{F}_p[A]^\times$ and so has order dividing $p^3 - 1$. As C has p-power order, this forces $C = I$, so that θ is conjugation by $((I - A)^{-1}\mathbf{d}, I)$. □

Proof of Theorem 25. First consider regular embeddings $\Gamma \to \mathrm{Hol}(G) = \mathrm{Hol}(H) \times \mathrm{Hol}(\mathbb{Z}_q)$ where $G = H \times \mathbb{Z}_q$ for some group H of order p^3. As $(p, q(q-1)) = 1$, the subgroup $\mathbb{Z}_{p^3}$ of Γ must embed as a regular subgroup of $\mathrm{Hol}(H)$. We know from [Ko98] that there are p^2 equivalence classes of such embeddings if $H = \mathbb{Z}_{p^3}$ and none otherwise. Moreover, if $H = \mathbb{Z}_{p^3}$ then $(q, |\mathrm{Hol}(H)|) = 1$, so the subgroup $\mathbb{Z}_q$ must embed as a regular subgroup of $\mathrm{Hol}(\mathbb{Z}_q)$, and there is only one equivalence class of such embeddings. This gives us p^2 Hopf–Galois structures, all of type Γ.

By Proposition 31, it only remains to show that there are no regular embeddings $\Gamma \to \mathrm{Hol}(G)$ when G is a nonabelian group of the form $G = H \rtimes \mathbb{Z}_q$ with $H = \mathbb{Z}_p^3$. But if $\Omega \in \mathrm{Hol}(G) = \rho(G) \rtimes \mathrm{Aut}(G)$ has p-power

order, then $\Omega^p \in \rho(G)$ by Proposition 32, so that in fact $\Omega^p \in \rho(H)$ and $\Omega^{p^2} = 1$. Hence Γ cannot embed in $\mathrm{Hol}(G)$. □

We note that groups of order p^3q were studied exhaustively in [We98].

References

[By96] Byott, N. P. Uniqueness of Hopf–Galois structure for separable field extensions. *Comm. Algebra* **24** (1996), no. 10, 3217–3228. MR1402555 (97j:16051a), Zbl 0878.12001, doi: 10.1080/00927879608825743. Corrigendum: *Comm. Algebra* **24** (1996), no. 11, 3705. MR1405283 (97j:16051b).

[By02] Byott, Nigel P. Integral Hopf–Galois structures on degree p^2 extensions of p-adic fields. *J. Algebra* **248** (2002), no. 1, 334–365. MR1879021 (2002j:11142), Zbl 0992.11065, doi: 10.1006/jabr.2001.9053.

[By04] Byott, Nigel P. Hopf–Galois structures on Galois field extensions of degree pq. *J. Pure Appl. Algebra* **188** (2004), no. 1–3, 45–57. MR2030805 (2004j:16041), Zbl 1047.16022, doi: 10.1016/j.jpaa.2003.10.010.

[By04b] Byott, Nigel P. Hopf–Galois structures on field extensions with simple Galois groups. *Bull. London Math. Soc.* **36** (2004), no. 1, 23–29. MR2011974 (2004i:16049), Zbl 1038.12002, doi: 10.1112/S0024609303002595.

[By07] Byott, Nigel P. Hopf–Galois structures on almost cyclic field extensions of 2-power degree. *J. Algebra* **318** (2007), no. 1, 351–371. MR2363137 (2009a:12006), Zbl 1183.12002, doi: 10.1016/j.jalgebra.2007.04.010.

[By12] Byott, N. P. Nilpotent and abelian Hopf–Galois structures on field extensions. Preprint, 2012.

[CaC99] Carnahan, Scott; Childs, Lindsay. Counting Hopf Galois structures on non-abelian Galois field extensions. *J. Algebra* **218** (1999), no. 1, 81–92. MR1704676 (2000e:12010), Zbl 0988.12003, doi: 10.1006/jabr.1999.7861.

[Ch00] Childs, Lindsay N. Taming wild extensions: Hopf algebras and local Galois module theory. Mathematical Surveys and Monographs, 80. *American Mathematical Society, Providence, RI*, 2000. viii+215 pp. ISBN: 0-8218-2131-8. MR1767499 (2001e:11116), Zbl 0944.11038.

[Ch03] Childs, Lindsay N. On Hopf Galois structures and complete groups. *New York J. Math.* **9** (2003), 99–115. MR2016184 (2004k:16097), Zbl 1038.12003.

[Ch11] Childs, Lindsay N. Fixed-point free endomorphisms and Hopf Galois structures. *Proc. Amer. Math. Soc.* To appear.

[CCo07] Childs, Lindsay N.; Corradino, Jesse. Cayley's theorem and Hopf Galois structures for semidirect products of cyclic groups. *J. Algebra* **308** (2007), no. 1, 236–251. MR2290920 (2007j:20026), Zbl 1119.16037, doi: 10.1016/j.jalgebra.2006.09.016.

[Di05] Dickson, Leonard Eugene. Definitions of a group and a field by independent postulates. *Trans. Amer. Math. Soc.* **6** (1905), no. 2, 198–204. MR1500706, Zbl 36.0207.01, doi: 10.1090/S0002-9947-1905-1500706-2.

[DF99] Dummit, David S.; Foote, Richard M. Abstract Algebra. Second edition. *John Wiley & Sons, New York*, 1999. Zbl 0943.00001.

[FCC12] Featherstonhaugh, S. C.; Caranti, A.; Childs, L. N. Abelian Hopf Galois structures on prime-power Galois field extensions. *Trans. Amer. Math. Soc.* **364** (2012), no. 7, 3675–3684. MR2901229, 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 (88i:12006),Zbl 0615.12026, doi: 10.1016/0021-8693(87)90029-9.

[Ko98] Kohl, Timothy. Classification of the Hopf Galois structures on prime power radical extensions. *J. Algebra* **207** (1998), no. 2, 525–546. MR1644203 (99g:16049), Zbl 0953.12003, doi: 10.1006/jabr.1998.7479.

[Ko11] Kohl, Timothy Regular permutation groups of order *mp*. Preprint, 2011.

[Pi82] Pierce, Richard S. Associative algebras. Graduate Texts in Mathematics, 88. *Springer-Verlag, New York-Berlin*, 1982. xii+436 pp. ISBN: 0-387-90693-2. MR0674652 (84c:16001), Zbl 0497.16001.

[We98] Western, A. E. Groups of order p^3q. *Proc. London Math. Soc.* **S1-30** (1898), no. 1, 209–263. MR1575465, JFM 30.0145.04, doi: 10.1112/plms/s1-30.1.209.

College of Engineering, Mathematics and Physical Sciences, University of Exeter, Exeter EX4 4QF, UK
N.P.Byott@ex.ac.uk

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

This paper is available via http://nyjm.albany.edu/j/2012/18-38.html.