COUNTING HOPF-GALOIS STRUCTURES ON CYCLIC FIELD EXTENSIONS OF SQUAREFREE DEGREE

ALI A. ALABDALI AND NIGEL P. BYOTT

Abstract. We investigate Hopf-Galois structures on a cyclic field extension L/K of squarefree degree n. By a result of Greither and Pareigis, each such Hopf-Galois structure corresponds to a group of order n, whose isomorphism class we call the type of the Hopf-Galois structure. We show that every group of order n can occur, and we determine the number of Hopf-Galois structures of each type. We then express the total number of Hopf-Galois structures on L/K as a sum over factorisations of n into three parts. As examples, we give closed expressions for the number of Hopf-Galois structures on a cyclic extension whose degree is a product of three distinct primes. (There are several cases, depending on congruence conditions between the primes.) We also consider one case where the degree is a product of four primes.

1. Introduction and Statement of Results

Let L/K be a finite Galois extension of fields with Galois group Γ. Then the group algebra $K[\Gamma]$ is a K-Hopf algebra, and its action on L endows L/K with a Hopf-Galois structure. In general, this is one among many possible Hopf-Galois structures on L/K. Greither and Pareigis [GP87] showed that these Hopf-Galois structures correspond to certain regular subgroups G in the group $\mathrm{Perm}(\Gamma)$ of permutations of the underlying set of Γ. Finding all Hopf-Galois structures in any particular case then becomes a combinatorial question in group theory. The groups Γ and G necessarily have the same order, but need not be isomorphic. We refer to the isomorphism type of G as the type of the corresponding Hopf-Galois structure.

Date: September 5, 2017.

1991 *Mathematics Subject Classification.* 12F10, 16T05.

Key words and phrases. Hopf-Galois structures; field extensions; groups of squarefree order.

The first-named author acknowledges support from The Higher Committee for Education Development in Iraq.

There is a substantial literature on Hopf-Galois structures on various classes of field extension. We mention a few results now, and some others in the final section of this paper. Let p be an odd prime. A cyclic field extension of degree p^m admits precisely p^{m-1} Hopf-Galois structures, all of cyclic type [Koh98]. An elementary abelian extension of degree p^m admits many more: there are at least $p^{m(m-1)-1}(p-1)$ Hopf-Galois structures of elementary abelian type if $p > m$ [Chi05], and there are also some of nonabelian type if $m \geq 3$ [BC12]. For a Galois extension whose Galois group Γ is abelian, the type G of any Hopf-Galois structure must be soluble [Byo15], although for a soluble, nonabelian Galois group Γ there can be Hopf-Galois structures whose type is not soluble. Recently, Crespo, Rio and Vela [CRV16] have investigated those Hopf-Galois structures on an extension L/K which arise by combining Hopf-Galois structures on L/F and on F/K for some intermediate field F.

In this paper, we investigate Hopf-Galois structures on cyclic extensions L/K of arbitrary squarefree degree. Thus we consider cyclic extensions whose degree has a prime factorisation at the other extreme to those treated in [Koh98]. We intend to discuss Hopf-Galois structures on arbitrary Galois extensions of squarefree degree in a future paper.

The type of a Hopf-Galois structure on a cyclic extension of squarefree degree n could potentially be any group G of order n. There may be many of these. Indeed, Hölder [Höl95] showed that the number of isomorphism types of groups of squarefree order n is given by

$$\sum_{de=n} \prod_{p|d} \left(\frac{p^{v(p,e)} - 1}{p-1} \right), \tag{1}$$

where the sum is over ordered pairs (d, e) of positive integers such that $de = n$, the product is over primes p dividing d, and $v(p, e)$ is the number of distinct prime factors q of e with $q \equiv 1 \pmod{p}$. It is clear that, as n varies over all squarefree integers, the expression (1) can become arbitrarily large.

It is an immediate consequence of Theorem 1 below that, for each group G of order n, the number of Hopf-Galois structures of type G on a cyclic extension of degree n cannot be zero. Thus all possible types do in fact occur. The cyclic extensions of squarefree degree therefore form a class for which both the number of distinct types of Hopf-Galois structures on a given extension, and the number of distinct prime factors of the degree of a given extension, may be arbitrarily large. To the best of our knowledge, this is the first class of extensions with these properties for which it has been possible to enumerate all Hopf-Galois structures. For comparison, we mention that, when the Galois group Γ is a nonabelian simple group, the number of prime factors of $|\Gamma|$ may be arbitrarily large, but there are only two Hopf-Galois structures, both of type Γ [Byo04a]. On the other hand, for Galois extensions of degree $p_1p_2p_3$, where p_1, p_2, p_3 are distinct odd primes satisfying certain congruence conditions, Kohl [Koh16] has determined all Hopf-Galois structures for each possible Galois group. In this case, the number of distinct types may be arbitrarily large, but the number of primes dividing the degree is of course fixed at three.

We will see in Proposition 3.5 that each group G of squarefree order n gives rise to a factorisation $n = dgz$ of n, in which g (respectively, z) is the order of the commutator subgroup G' (respectively, the centre $Z(G)$) of G. We can now state the first of our two main results.

Theorem 1. *Let L/K be a cyclic extension of fields of squarefree degree n, and let G be any group of order n. Let $z = |Z(G)|$, $g = |G'|$ and $d = n/(gz)$. Then L/K admits precisely $2^{\omega(g)}\varphi(d)$ Hopf-Galois structures of type G, where φ is Euler's totient function and $\omega(g)$ is the number of (distinct) prime factors of g.*

Our second result gives the total number of Hopf-Galois structures.

Theorem 2. *The number of Hopf-Galois structures on a cyclic field extension of squarefree degree n is*

$$\sum_{dgz=n} 2^{\omega(g)}\mu(z)\prod_{p|d}\left(p^{v(p,g)}-1\right), \tag{2}$$

where the product is over ordered triples (d, g, z) of natural numbers with $dgz = n$. Here μ is the Möbius function.

We remark that (2) has a similar shape to Hölder's formula (1), although with a sum over factorisations into three parts rather than two. In both cases, the term for each factorisation involves a product over primes p dividing d, in which the contribution corresponding to p does not depend on d and p alone. (In (1) it depends on e, and in (2) on g.)

2. Preliminaries on Hopf-Galois structures

Let L/K be a field extension of finite degree, and let H be a cocommutative K-Hopf algebra acting on L . We write $\Delta\colon H \to H \otimes_K H$ and $\epsilon\colon H \to K$ for the comultiplication and counit maps on H, and use Sweedler's notation $\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)}$. We will say that the action of H on L makes L into an H-module algebra if $h \cdot (xy) =$

$\sum_{(h)}(h_{(1)}\cdot x)\otimes(h_{(2)}\cdot y)$ and $h\cdot k=\epsilon(h)k$ for all $h\in H$, all x, $y\in L$ and all $k\in K$. A Hopf-Galois structure on L consists of a Hopf algebra H acting on L so that L is an H-module algebra and the K-linear map $\theta\colon L\otimes_K L\to \mathrm{Hom}_K(H,L)$ is bijective, where $\theta(x\otimes y)(h)=x(h\cdot y)$ for x, $y\in L$ and $h\in H$.

When L/K is separable, Greither and Pareigis [GP87] used descent theory to show how all Hopf-Galois structures on L/K could be described in group-theoretic terms. We consider here only the special case where L/K is a Galois extension in the classical sense (that is, L/K is normal as well as separable). Let $\Gamma=\mathrm{Gal}(L/K)$ be the Galois group of L/K. Then the Hopf-Galois structures on L/K correspond bijectively to subgroups G of $\mathrm{Perm}(\Gamma)$ which are regular on Γ and are normalised by the group $\lambda(\Gamma)$ of left translations by elements of Γ. Recall that a group G acting on a set X is regular if the action is transitive on X and the stabiliser of any point is trivial.

The direct determination of all regular subgroups in $\mathrm{Perm}(\Gamma)$ normalised by $\lambda(\Gamma)$ is often difficult as the group $\mathrm{Perm}(\Gamma)$ is large. However, the condition that $\lambda(\Gamma)$ normalises G means that Γ is contained in the holomorph $\mathrm{Hol}(G)=G\rtimes\mathrm{Aut}(G)$ of G, where the latter group is viewed as a subgroup of $\mathrm{Perm}(\Gamma)$ and is usually much smaller than $\mathrm{Perm}(\Gamma)$. We may then view Γ as acting on G, and this action is again regular. If the isomorphism types of groups G^* of order $|\Gamma|$ admit a manageable classification, the Hopf-Galois structures on L/K can be determined by considering each G^* in turn and finding the regular subgroups Γ^* of $\mathrm{Hol}(G^*)$ which are isomorphic to Γ. This leads to the following result, cf. [Byo96, Cor. to Prop. 1] or [Chi00, §7]:

Lemma 2.1. *Let L/K be a finite Galois extension of fields with Galois group Γ, and, for any group G with $|G|=|\Gamma|$, let $e'(G,\Gamma)$ be the number of regular subgroups of $\mathrm{Hol}(G)$ isomorphic to Γ. Then the number $e(G,\Gamma)$ of Hopf-Galois structures on L/K of type G is given by*

$$e(G,\Gamma)=\frac{|\mathrm{Aut}(\Gamma)|}{|\mathrm{Aut}(G)|}\,e'(G,\Gamma).$$

Moreover, the total number of Hopf-Galois structures on L/K is given by $\sum_G e(G,\Gamma)$, where the sum is over all isomorphism types G of groups of order $|\Gamma|$.

3. Preliminaries on groups of squarefree order

We will call a finite group a C-group if all its Sylow subgroups are cyclic. In particular, any group of squarefree order is a C-group. All C-groups are metabelian, so C-groups can in principle be classified

[Rob96, 10.1.10]. This classification is given in a rather explicit form in a paper of Murty and Murty [MM84], who investigated the asymptotic behaviour of the number of C-groups of order up to a given bound. We state their classification result, in the special case of groups of squarefree order, as Lemma 3.2 below.

Notation 3.1. For an integer $N \geq 1$, we denote by $\mathbb{Z}_N$ the ring $\mathbb{Z}/N\mathbb{Z}$ of integers modulo N, and by $U(N)$ the group of units in $\mathbb{Z}_N$. We write $\mathrm{ord}_N(a)$ for the order of an element $a \in U(N)$. Abusing notation, we will often use the same symbol for an element of $\mathbb{Z}$ and its class in $\mathbb{Z}_N$. We write 1_G for the identity element of a group G.

Lemma 3.2. *Let n be squarefree. Then any group of order n has the form*

$$G(d, e, k) = \langle \sigma, \tau \colon \sigma^e = \tau^d = 1_G, \tau\sigma\tau^{-1} = \sigma^k \rangle$$

where $n = de$, $\gcd(d, e) = 1$ and $\mathrm{ord}_e(k) = d$. Conversely, any choice of d, e and k satisfying these conditions gives a group $G(d, e, k)$ of order n. Moreover, two such groups $G(d, e, k)$ and $G(d', e', k')$ are isomorphic if and only if $d = d'$, $e = e'$, and k, k' generate the same cyclic subgroup of $U(e)$.

Proof. This follows from [MM84, Lemmas 3.5 & 3.6]. $\square$

Remark 3.3. The existence of k with $\mathrm{ord}_e(k) = d$ implies that d divides $\varphi(e) = |U(e)|$. Thus there may be many factorisations $n = de$ of n for which no groups $G(d, e, k)$ occur.

Remark 3.4. We note in passing how Hölder's formula (1) follows from Lemma 3.2. For fixed d and e, the number of isomorphism types of group $G(d, e, k)$ is the number of (necessarily cyclic) subgroups of order d in $U(e)$. Each such group is the product of its Sylow p-subgroups for the primes p dividing d. For each such p, the p-rank of $U(e)$ is $v(p, e)$, so $U(p)$ contains $(p^{v(p,e)} - 1)/(p - 1)$ subgroups of order p. Taking the product over p gives the number of subgroups of order d. Summing over d yields the formula (1) for the number of isomorphism types of groups of order n.

Proposition 3.5. *Let $G = G(d, e, k)$ be a group of squarefree order n as in Lemma 3.2. Let $z = \gcd(e, k - 1)$ and $g = e/z$, so that we have factorisations $e = gz$ and $n = de = dgz$. Then the centre $Z(G)$ of G is the cyclic group $\langle \sigma^g \rangle$ of order z, and the commutator subgroup G' of G is the the cyclic group $\langle \sigma^z \rangle$ of order g.*

Proof. For $\gamma = \sigma^a\tau^b \in G$, we have $\sigma^{-1}\gamma\sigma = \sigma^{a-1+k^b}\tau^b$. Since $\mathrm{ord}_e(k) = d$, it follows that γ commutes with σ if and only if $d \mid b$. But then

$\gamma = \sigma^a$ and $\tau\gamma\tau^{-1} = \tau\sigma^a\tau^{-1} = \sigma^{ak}$. Thus $\tau\gamma\tau^{-1} = \gamma$ precisely when $e \mid a(k-1)$, that is, when $g \mid a$. Hence $Z(G) = \langle \sigma^g \rangle$.

Turning to G', we have $\tau\sigma\tau^{-1}\sigma^{-1} = \sigma^{k-1}$. Thus G' contains the normal subgroup $\langle \sigma^{k-1} \rangle = \langle \sigma^z \rangle$ of G. Equality holds since $G/\langle \sigma^{k-1} \rangle$ is abelian. □

We next find the number of isomorphism classes of groups G corresponding to the factorisation $n = dgz$.

Proposition 3.6. *Let $n = dgz$ be squarefree. Then the number of isomorphism types of groups G of order n with $|Z(G)| = z$ and $|G'| = g$ is*

$$\varphi(d)^{-1} \sum_{f \mid g} \mu\left(\frac{g}{f}\right) \prod_{p \mid d} (p^{v(p,f)} - 1). \tag{3}$$

Proof. We keep d and $e = n/d$ fixed. For each factor g of e let $m(g)$ be the number of isomorphism types of groups $G = G(d, e, k)$ (with k varying) for which $|G'| = g$. We need to show that $m(g)$ is given by the formula (3).

Let $m^*(g)$ be the number of groups $G(d, e, k)$ for which $|G'|$ *divides* g. Then

$$m^*(g) = \sum_{f \mid g} m(f),$$

and so, by Möbius inversion,

$$m(g) = \sum_{f \mid g} m^*(f) \mu\left(\frac{g}{f}\right). \tag{4}$$

The distinct isomorphism types of groups G correspond to distinct subgroups D of order d in $U(e) \cong \prod_{q \mid e} U(q)$, where the product is over primes q dividing e. Let $f \mid e$. Then $|G'|$ divides f precisely when e/f divides $|Z(G)|$, which occurs when D has trivial projection in the factor $U(q)$ for each prime q dividing e/f. Hence $m^*(f)$ is the number of subgroups of order d in $U(f)$, and, arguing as in Remark 3.4, this is $\prod_{p \mid d}(p^{v(p,f)} - 1)/(p-1)$. Substituting into (4) and noting that $\prod_{p \mid d}(p-1) = \varphi(d)$, we obtain the expression (3) for $m(g)$. □

4. Automorphisms and the Holomorph

For this section and the next, we fix a group $G = G(d, e, k)$ of squarefree order n. We keep the preceding notation, so $g = |G'|$, $z = |Z(G)|$, and $n = de = dgz$. Our goal is to find the number of cyclic subgroups of $\mathrm{Hol}(G)$ which are regular on G. By Lemma 2.1, this will enable us to find the number of Hopf-Galois structures of type G on a cyclic extension of degree n. In this section, we will describe $\mathrm{Aut}(G)$ and $\mathrm{Hol}(G)$. In §5, we determine all regular cyclic subgroups in $\mathrm{Hol}(G)$ and complete the proof of Theorem 1. In §6, we sum over the different isomorphism types G to prove Theorem 2.

Until the end of §6, we shall systematically use the notation p for prime factors of d and q for prime factors of e. Thus the primes q are of two types: either $q \mid g$ or $q \mid z$.

We begin by recording a formula which allows us to perform calculations in G itself. For integers h and $j \geq 0$, we define

$$S(h,j) = \sum_{i=0}^{j-1} h^i. \tag{5}$$

In particular, $S(h,0) = 0$. A simple induction shows that, for any $a \in \mathbb{Z}$,

$$(\sigma^a \tau)^j = \sigma^{aS(k,j)} \tau^j. \tag{6}$$

The next result describes the automorphisms of G.

Lemma 4.1. *We have* $|\mathrm{Aut}(G)| = g\varphi(e)$ *and*

$$\mathrm{Aut}(G) \cong C_g \rtimes U(e),$$

where $a \in U(e)$ *acts on* C_g *by* $x \mapsto x^a$. *(Note that in general this action is not faithful.)*

Explicitly, $\mathrm{Aut}(G)$ *is generated by the automorphism* θ *and automorphisms* ϕ_s *for each* $s \in U(e)$, *where*

$$\theta(\sigma) = \sigma, \qquad \theta(\tau) = \sigma^z \tau, \tag{7}$$

and

$$\phi_s(\sigma) = \sigma^s, \qquad \phi_s(\tau) = \tau. \tag{8}$$

These automorphisms satisfy the relations

$$\theta^g = \mathrm{id}_G, \qquad \phi_s\phi_t = \phi_{st}, \qquad \phi_s\theta\phi_s^{-1} = \theta^s. \tag{9}$$

Proof. We first verify the existence of the automorphisms θ and ϕ_s. Since $(\sigma^z\tau)\sigma(\sigma^z\tau)^{-1} = \sigma^k$, (7) will determine an automorphism θ provided that $\sigma^z\tau$ has order d. By (6), this will hold if $e \mid zS(k,d)$, that is, if $g \mid S(k,d)$. But for each prime $q \mid g$, we have $k^d \equiv 1 \not\equiv k \pmod q$, so that

$$S(k,d) = \frac{k^d - 1}{k - 1} \equiv 0 \pmod q.$$

Thus $g \mid S(k,d)$, as required. This shows the existence of the automorphism θ. For $s \in U(e)$, the element σ^s has order e and $\tau\sigma^s\tau^{-1} = (\sigma^s)^k$. It follows that there is an automorphism ϕ_s as given in (8).

It is clear that θ has order g. The remaining relations in (9) are easily verified by checking them on the generators σ, τ of G.

We have now shown that θ and the ϕ_s generate a subgroup of $\mathrm{Aut}(G)$ isomorphic to $C_g \rtimes U(e)$. This subgroup has order $g\varphi(e)$. It remains to show that there are no further automorphisms.

Let $\psi \in \mathrm{Aut}(G)$. As $\langle\sigma\rangle$ is a characteristic subgroup of G, being the unique subgroup of order e, we have $\psi(\sigma) = \sigma^s$ for some $s \in U(e)$. Let $\psi(\tau) = \sigma^a\tau^b$ with $0 \le b < d$. Since ψ must satisfy $\psi(\tau)\psi(\sigma)\psi(\tau)^{-1} = \psi(\sigma)^k$, we have $\sigma^{sk^b} = \sigma^{sk}$ and hence $b = 1$. Thus, by (6) again,

$$\psi(\tau)^d = \sigma^{aS(k,d)},$$

so that $aS(k,d) \equiv 0 \pmod{e}$. In particular, for each prime q dividing z, we have $q \mid aS(k,d)$. But $S(k,d) \equiv d \not\equiv 0 \pmod{q}$ since $k \equiv 1 \pmod{q}$. Thus $q \mid a$. It follows that $a = zc$ for some $c \in \mathbb{Z}$, so $\psi = \theta^c\phi_s$. □

We now consider the holomorph $\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G)$ of G. We write an element of this group as $[\alpha, \psi]$, where $\alpha \in G$ and $\psi \in \mathrm{Aut}(G)$. The multiplication in $\mathrm{Hol}(G)$ is given by

$$[\alpha,\psi][\alpha',\psi'] = [\alpha\psi(\alpha'), \psi\psi']. \tag{10}$$

(The subgroup G in $\mathrm{Hol}(G)$ is therefore identified with the left translations in $\mathrm{Perm}(G)$.) In view of Lemma 4.1, an arbitrary $x \in \mathrm{Hol}(G)$ can be written $x = [\sigma^a\tau^b, \theta^c\phi_s]$, where $a \in \mathbb{Z}_e$, $s \in U(e)$, $b \in \mathbb{Z}_d$ and $c \in \mathbb{Z}_g$. In Lemma 4.2 below, we will give a formula for powers of x in the special case $b = 1$. We will then show in Proposition 4.3 why this case is all we need. We first introduce some further notation.

Define

$$T(k,s,j) = \sum_{h=0}^{j-1} S(s,h)k^{h-1} \text{ for } j \ge 1, \qquad T(k,s,0) = 0, \tag{11}$$

where $S(s,h)$ is given by (5). Note that we then have $T(k,s,1) = 0$ and

$$T(k,s,j+1) = T(k,s,j) + k^{j-1}S(s,j) \text{ for } j \ge 0.$$

Lemma 4.2. *Let $x = [\sigma^a\tau, \theta^c\phi_s]$. Then, for $j \ge 0$, we have*

$$x^j = [\sigma^{A(j)}\tau^j, \theta^{cS(s,j)}\phi_{s^j}] \tag{12}$$

where $A(j) = aS(sk,j) + czkT(k,s,j)$.

Proof. We argue by induction on j. When $j = 0$, we have $S(s,0) = T(k,s,0) = 0$ and $A(0) = 0$, so (12) holds in this case. Assuming (12) for j, we have from (10) that

$$\begin{aligned} x^{j+1} &= [\sigma^{A(j)}\tau^j, \theta^{cS(s,j)}\phi_{s^j}][\sigma^a\tau, \theta^c\phi_s] \\ &= [\sigma^{A(j)}\tau^j(\theta^{cS(s,j)}\phi_{s^j}(\sigma^a\tau)), \theta^{cS(s,j)}\phi_{s^j}\theta^c\phi_s]. \end{aligned}$$

Thus, using (9), the second component of x^{j+1} is

$$\theta^{cS(s,j)}\phi_{s^j}\theta^c\phi_s = \theta^{cS(s,j)}\theta^{cs^j}\phi_{s^j}\phi_s = \theta^{cS(s,j+1)}\phi_{s^{j+1}},$$

as required for (12). As for the first component of x^{j+1}, since

$$\theta^{cS(s,j)}\phi_{s^j}(\sigma^a\tau) = \sigma^{as^j}\sigma^{czS(s,j)}\tau,$$

we have

$$\begin{aligned} \sigma^{A(j)}\tau^j(\theta^{cS(s,j)}\phi_{s^j}(\sigma^a\tau)) &= \sigma^{A(j)}\tau^j\sigma^{as^j}\sigma^{czS(s,j)}\tau \\ &= \sigma^{A(j)}\sigma^{as^jk^j}\sigma^{czS(s,j)k^j}\tau^{j+1}. \end{aligned}$$

We write this as $\sigma^{A'}\tau^{j+1}$, and calculate

$$\begin{aligned} A' &= A(j) + as^jk^j + czS(s,j)k^j \\ &= a(S(sk,j) + (sk)^j) + czk[T(k,s,j) + k^{j-1}S(s,j)] \\ &= aS(sk,j+1) + czkT(k,s,j+1) \\ &= A(j+1). \end{aligned}$$

Thus (12) holds with j replaced by $j+1$. This completes the induction. □

Proposition 4.3. *Let C be a cyclic subgroup of* $\mathrm{Hol}(G)$ *which is regular on G. Then C is generated by some element*

$$x = [\sigma^a\tau, \theta^c\phi_s],$$

in which τ occurs with exponent 1*. In fact, C contains precisely $\varphi(e)$ generators of this type.*

Proof. For any $\psi \in \mathrm{Aut}(G)$ and arbitrary $\alpha = \sigma^a\tau^b \in G$, we have $\psi(\alpha) = \sigma^{a'}\tau^b$ for some $a' \in \mathbb{Z}$. This is clear from Lemma 4.1 as it holds for $\psi = \phi_s$ and $\psi = \theta$. It then follows from (10) that the function $\mathrm{Hol}(G) \to \langle\tau\rangle$, given by $[\sigma^a\tau^b, \psi] \mapsto \tau^b$, is a group homomorphism. (This is not automatic, since the function $\mathrm{Hol}(G) \to G$ given by $[\sigma^a\tau^b, \psi] \mapsto \sigma^a\tau^b$, is not in general a homomorphism.) In particular, for any $x = [\sigma^a\tau^b, \theta^c\phi_s] \in \mathrm{Hol}(G)$ and any $j \geq 1$, we have $x^j = [\sigma^A\tau^{bj}, \psi]$ for some $A \in \mathbb{Z}_e$ and some $\psi \in \mathrm{Aut}(G)$, both depending on j. The permutation x^j of G takes 1_G to $\sigma^A\tau^{bj}$.

Now let C be a regular cyclic subgroup of $\mathrm{Hol}(G)$, and let $x = [\sigma^a\tau^b, \theta^c\phi_s]$ be a generator. Thus x has order n. Since C is transitive on G, the elements $\sigma^A\tau^{bj}$, as j varies, must run through all elements of G. In particular, bj must run through all residue classes modulo d. Hence $\gcd(b,d)=1$, and there exists $f \geq 1$ with $bf \equiv 1 \pmod{d}$. Since $\gcd(d,e)=1$, we may further assume that $\gcd(f,e)=1$. Then $\gcd(f,n)=1$, so that x^f is also a generator of C, and $x^f = [\sigma^{A'}\tau^{bf}, \psi'] = [\sigma^{A'}\tau, \psi']$ for some A' and ψ'. Replacing x by x^f, we have found a generator of C with $b=1$, as required.

Now let x be any such generator. Then x^j will be another if and only if $\gcd(j,n)=1$ and $j \equiv 1 \pmod{d}$. The number of such generators is therefore $\varphi(n)/\varphi(d) = \varphi(e)$. □

5. Hopf-Galois structures of type G

As a first step towards determining when the element x in Proposition 4.3 generates a regular subgroup, we give a condition for transitivity.

Lemma 5.1. *Let $x = [\sigma^a\tau, \theta^c\phi_s] \in \mathrm{Hol}(G)$. Then the subgroup $\langle x\rangle$ of $\mathrm{Hol}(G)$ acts transitively on G if and only if $\langle x^d\rangle$ acts transitively on $\langle\sigma\rangle$.*

Proof. Let $\langle x\rangle$ be transitive on G. Then, for each $i \in \mathbb{Z}$, there is some j such $x^j \cdot 1_G = \sigma^i$. Then $d \mid j$ by (12). Thus $\langle x^d\rangle$ acts transitively on $\langle\sigma\rangle$. Conversely, suppose that $\langle x^d\rangle$ acts transitively on $\langle\sigma\rangle$. Let $\sigma^i\tau^j \in G$. By Lemma 4.2, we have $x^{-j}\cdot\sigma^i\tau^j \in \langle\sigma\rangle$. As $\langle x^d\rangle$ is transitive on $\langle\sigma\rangle$, there is some $h \in \mathbb{Z}$ with $x^{dh-j}\cdot\sigma^i\tau^j = 1_G$. Thus the arbitrary element $\sigma^i\tau^j$ lies in the same orbit under $\langle x\rangle$ as 1_G, so that $\langle x\rangle$ is transitive on G. □

In order to study the orbits of $\langle x^d\rangle$ on $\langle\sigma\rangle$, we examine the congruence properties of the sums $S(k,j)$ and $T(k,s,j)$ defined in (5) and (11) when j is a multiple of d.

Proposition 5.2. *Let q be a prime dividing e. In the following, all congruences are modulo q. We will omit the modulus for brevity. Abusing notation, we will write $\frac{u}{v}$ in such a congruence to denote uv^* where $vv^* \equiv 1$. (This notation will only be used when $v \not\equiv 0$.)*

(i) *For any s, $i \in \mathbb{Z}$ with $i \geq 0$, we have*

$$S(s,di) \equiv \begin{cases} di & \text{if } s \equiv 1; \\ \dfrac{s^{di}-1}{s-1} & \text{otherwise.} \end{cases}$$

(ii) *Recall that* $k^d \equiv 1$. *If also* $k \not\equiv 1$ *then, for any* s, $i \in \mathbb{Z}$ *with* $i \geq 0$, *we have*

$$T(k,s,di) \equiv \begin{cases} \dfrac{di}{k(k-1)} & \text{if } s \equiv 1; \\[2ex] \dfrac{di}{k(s-1)} & \text{if } sk \equiv 1; \\[2ex] \dfrac{(s^{di}-1)}{k(s-1)(sk-1)} & \text{otherwise.} \end{cases}$$

Proof. (i) This is immediate.

(ii) The case $i = 0$ is clear, so assume $i \geq 1$. First let $s \equiv 1$. Then $S(s,j) \equiv j$, so

$$\begin{aligned} (k-1)T(k,s,di) &= \sum_{j=0}^{di-1} (k-1)jk^{j-1} \\ &= \sum_{j=0}^{di-1} jk^j - \sum_{j=1}^{di-1} jk^{j-1} \\ &= \sum_{j=0}^{di-1} jk^j - \sum_{j=0}^{di-2} (j+1)k^j \\ &= \sum_{j=0}^{di-1} jk^j - \sum_{j=0}^{di-1} (j+1)k^j + dik^{di-1} \\ &= -\sum_{j=0}^{di-1} k^j + dik^{di-1}. \end{aligned}$$

As $k^d \equiv 1 \not\equiv k$, we then have

$$(k-1)T(k,s,di) \equiv dik^{di-1},$$

giving the result for $s \equiv 1$.

If $s \not\equiv 1$ then

$$\begin{aligned} T(k,s,di) &\equiv \sum_{j=0}^{di-1} \left(\frac{s^j - 1}{s-1} \right) k^{j-1} \\ &\equiv \frac{1}{k(s-1)} \left[\sum_{j=0}^{di-1} (sk)^j - \sum_{j=0}^{di-1} k^j \right]. \end{aligned}$$

The second sum vanishes mod q. The first is congruent to di if $sk \equiv 1$, giving the result in this case. Finally if $sk \not\equiv 1 \not\equiv s$ then

$$\begin{aligned} T(k,s,di) &\equiv \frac{1}{k(s-1)} \sum_{j=0}^{di-1} (sk)^j \\ &\equiv \frac{1}{k(s-1)(sk-1)} \left((sk)^{di} - 1 \right) \\ &\equiv \frac{1}{k(s-1)(sk-1)} \left(s^{di} - 1 \right). \end{aligned}$$

□

Lemma 5.3. *Let* $x = [\sigma^a \tau, \theta^c \phi_s] \in \mathrm{Hol}(G)$*, so* $a \in \mathbb{Z}_e$*,* $c \in \mathbb{Z}_g$*,* $s \in U(e)$*. Then* x *generates a regular cyclic subgroup of* $\mathrm{Hol}(G)$ *if and only if the triple* (s, a, c) *satisfies the following conditions:*

(i) *for each prime* $q \mid z$*, we have* $s \equiv 1 \pmod q$ *and* $q \nmid a$*;*
(ii) *for each prime* $q \mid g$*, either*

$$s \equiv 1 \pmod q \text{ and } c \not\equiv 0 \pmod q, \text{ or}$$

$$s \equiv k^{-1} \pmod q \text{ and } (s-1)a + cz \not\equiv 0 \pmod q.$$

Proof. Suppose that $\langle x \rangle$ is regular, and hence transitive, on G. By Lemma 5.1, $\langle x^d \rangle$ is transitive on $\langle \sigma \rangle$. It follows using Lemma 4.2 that the expression

$$A(di) = aS(sk, di) + czkT(k, s, di)$$

represents all residue classes mod e as i varies. In particular, $A(di)$ represents every residue class mod q for each prime factor q of e. We investigate this condition for each q in turn. Again, we omit the modulus in congruences modulo q.

First, let $q \mid z$, so $k \equiv 1$. If $s \not\equiv 1$, then $sk \not\equiv 1$, so by Proposition 5.2(i) we have

$$A(di) \equiv \frac{a(s^{di} - 1)}{s - 1},$$

which cannot represent all residue classes mod q since there is no i such that $s^{di} \equiv 0$. On the other hand, if $s \equiv 1$ then

$$A(di) \equiv adi. \tag{13}$$

Since $q \nmid d$, this represents all residue classes mod q precisely when $q \nmid a$. Thus (i) holds.

Now let $q \mid g$, so $k \not\equiv 1$ but $k^d \equiv 1$. If $s \not\equiv 1$ and $s \not\equiv k^{-1}$, then, using both parts of Proposition 5.2, we have

$$\begin{aligned} A(di) &\equiv \left(\frac{(sk)^{di}-1}{sk-1}\right) a + czk\left(\frac{s^{di}-1}{k(s-1)(sk-1)}\right) \\ &= \frac{(s^{di}-1)}{(s-1)(sk-1)}\left((s-1)a+cz\right). \end{aligned}$$

Again, this cannot represent all residue classes mod q since $s^{di} \not\equiv 0$.

It remains to consider the two special cases $s \equiv 1 \not\equiv k$ and $s \equiv k^{-1} \not\equiv 1$.

If $s \equiv 1 \not\equiv k$ then, as $(sk)^d \equiv k^d \equiv 1$, we have

$$A(di) \equiv czk\left(\frac{di}{k(k-1)}\right) = \frac{czdi}{k-1}. \tag{14}$$

As $q \nmid zd$, this represents all residue classes mod q precisely when $q \nmid c$, giving the first case in (ii).

If $s \equiv k^{-1} \not\equiv 1$ then

$$\begin{aligned} A(di) &\equiv adi + czk\left(\frac{di}{k(s-1)}\right) \\ &\equiv \frac{di}{s-1}\left((s-1)a+cz\right). \end{aligned} \tag{15}$$

This represents all residue classes mod q precisely when $(s-1)a+cz \not\equiv 0$, giving the second case in (ii).

We have now shown that if x generates a regular cyclic subgroup, then (i) and (ii) hold.

Conversely, suppose that (i) and (ii) hold. Then, by Proposition 5.2, the congruences (13), (14) and (15) hold modulo all relevant q. For each prime $q \mid e$, we then have that $A(di)$ represents all residue classes mod q as i runs through any complete set of residues mod q. By the Chinese Remainder Theorem, $A(di)$ then ranges through all residue classes mod e as i does. By Lemma 4.2, $\langle x^d \rangle$ is then transitive on $\langle \sigma \rangle$, so $\langle x \rangle$ is transitive on G by Lemma 5.1. Finally, (13), (14) and (15) show that $A(de) \equiv 0 \pmod{e}$, so that $x^n = 1_G$. Hence $\langle x \rangle$ is regular on G. □

Proof of Theorem 1. By Proposition 4.3, any regular cyclic subgroup of $\mathrm{Hol}(G)$ is generated by an element x as in Lemma 5.3. We count the number of triples (s, a, c) satisfying the conditions there. As there is only one possibility for $s \bmod q$ when $q \mid z$ but two when $q \mid g$, there are $2^{\omega(g)}$ possibilities for $s \pmod{e}$. Let us fix s and consider the possibilities for a and c. For each prime $q \mid z$, condition (i) in

Lemma 5.3 excludes one possibility for $a \bmod q$. For each $q \mid g$, we may choose $a \bmod q$ arbitrarily, and then, in either case of condition (ii), one possibility for $c \bmod q$ is excluded. Thus we have $\varphi(z)g$ choices for $a \bmod e$, and then $\varphi(g)$ choices for $c \bmod g$. The number of elements $x = [\sigma^a\tau, \theta^c\phi_s]$ which generate a regular subgroup is therefore $2^{\omega(g)}\varphi(z)g\varphi(g)$. By Proposition 4.3, each regular cyclic subgroup contains $\varphi(e) = \varphi(z)\varphi(g)$ such generators, so there are $2^{\omega(g)}g$ of these subgroups. Thus, using Lemma 2.1 and Lemma 4.1 (and writing C_n for the cyclic group of order n), we find that the number of Hopf-Galois structures of type G is

$$\frac{|\mathrm{Aut}(C_n)|}{|\mathrm{Aut}(G)|}\,2^{\omega(g)}g = \frac{\varphi(n)}{g\varphi(e)}2^{\omega(g)}g = 2^{\omega(g)}\varphi(d).$$

□

6. Proof of Theorem 2

In this section, we obtain the total number of Hopf-Galois structures on a cyclic field extension of squarefree degree n, thereby completing the proof of Theorem 2.

For each factorisation $n = dgz$, we have seen in Proposition 3.6 that the number of corresponding isomorphism types of group G is

$$\varphi(d)^{-1}\sum_{f\mid g}\mu\left(\frac{g}{f}\right)\prod_{p\mid d}(p^{v(p,f)}-1).$$

We have also seen in Theorem 1 that there $2^{\omega(g)}\varphi(d)$ Hopf-Galois structures of each of these types. To obtain the total number of Hopf-Galois structures, we simply multiply these two quantities and sum over factorisations of n. This yields

$$\sum_{dgz=n} 2^{\omega(g)}\varphi(d)\left(\varphi(d)^{-1}\sum_{f\mid g}\mu\left(\frac{g}{f}\right)\prod_{p\mid d}(p^{v(p,f)}-1)\right).$$

Setting $t = g/f$ and noting that $\omega(g) = \omega(t) + \omega(f)$, we can rewrite the previous sum as

$$\sum_{dftz=n}\mu(t)2^{\omega(t)}2^{\omega(f)}\prod_{p\mid d}(p^{v(p,f)}-1).$$

Let $m = tz$, and observe that $\mu(t) = (-1)^{\omega(t)}$. The sum then becomes

$$\sum_{dfm=n}\left(\sum_{t\mid m}(-2)^{\omega(t)}\right)2^{\omega(f)}\prod_{p\mid d}(p^{v(p,f)}-1).$$

Recall that a function F on the natural numbers is said to be multiplicative if $F(rs) = F(r)F(s)$ whenever $\gcd(r,s) = 1$. The function $t \mapsto (-2)^{\omega(t)}$ is clearly multiplicative, and hence so is the function $m \mapsto \sum_{t|m}(-2)^{\omega(t)}$. However, evaluating this last function at a prime q gives $(-2)^{\omega(1)} + (-2)^{\omega(q)} = 1 + (-2) = -1 = \mu(q)$. As μ is also multiplicative, it follows that $\sum_{t|m}(-2)^{\omega(t)} = \mu(m)$ for squarefree m. (This is not true for arbitrary natural numbers m.) Hence the total number of Hopf-Galois structures on a cyclic extension of squarefree degree n is

$$\sum_{dfm=n} \mu(m) 2^{\omega(f)} \prod_{p|d} (p^{v(p,f)} - 1).$$

After a change of notation, this gives the formula (2), completing the proof of Theorem 2.

7. Examples

In this section, we give some examples and show how several results in the literature can be obtained as special cases of our results. Throughout, n is a squarefree integer and L/K is a cyclic Galois extension of degree n.

7.1. **Cyclic Hopf-Galois Structures.** The group $G(d,e,k)$ in Lemma 3.2 is cyclic only when $d = 1$, $e = n$. Indeed, this is the only case where $G(d,e,k)$ is abelian, or even nilpotent. In this case $z = n$, $g = 1$, and Theorem 1 shows that there is only one Hopf-Galois structure of cyclic (or abelian, or nilpotent) type on L/K. This can also be seen from [Byo13, Theorem 2]. The unique cyclic Hopf-Galois structure is of course the classical one.

When $\gcd(n, \varphi(n)) = 1$, there are no other groups $G(d,e,k)$, and hence there are no Hopf-Galois structures on L/K beyond the classical one. This was shown, together with its converse, in [Byo96]. The case that n is prime occurs in [Chi89].

7.2. **Dihedral Hopf-Galois Structures.** Let $n = 2m$ where m is an odd squarefree number. The group $G(d,e,k)$ in Lemma 3.2 is dihedral when $d = 2$ and $k = -1 \in U(e)$. Then $e = g = m$. It follows from Theorem 1 that a cyclic extension of degree n admits $2^{\omega(m)}$ Hopf-Galois structures of dihedral type.

7.3. **Two Primes.** Let $n = pq$ for primes $p > q$. We assume that $q \mid (p-1)$ (since otherwise the only group of order n is the cyclic group C_n). Up to isomorphism, there are two groups of order n, the cyclic group C_n (with $d = 1$, $g = 1$, $e = z = pq$) and the metabelian

d	g	z	Term in (2)
1	pq	1	4
1	p	q	-2
1	q	p	-2
1	1	pq	1
q	p	1	$2(q-1)$

TABLE 1. Nonzero terms in (2) for $n = pq$.

group $M = C_p \rtimes C_q$ where C_q acts nontrivially on C_p (so $d = q$, $e = g = p$, $z = 1$). As we have seen in §7.1, a cyclic extension of degree n admits just one Hopf-Galois structure of cyclic type (namely the classical one). By Theorem 1, it also admits $2^{\omega(p)}\varphi(q) = 2(q-1)$ Hopf-Galois structures of type M. This result was obtained in [Byo04b], where we also considered Hopf-Galois structures on a Galois extension with Galois group M. When $q = 2$, the result follows from §7.2.

Let us also verify that Proposition 3.6 correctly counts the isomorphism types corresponding to each factorisation $n = dgz$, and that Theorem 2 correctly counts the total number of Hopf-Galois structures, in this case.

In the sum (3) of Proposition 3.6, $\prod_{p|d}(p^{v(p,f)} - 1)$ vanishes unless $d = 1$ or $d = q$, $f = p$ (so that also $g = p$). When $d = 1$, (3) reduces to

$$\sum_{f|g} \mu\left(\frac{g}{f}\right) = \begin{cases} 1 & \text{if } g = 1; \\ 0 & \text{otherwise.} \end{cases}$$

Thus when $d = 1$, to get a group $G(d,e,k)$ we must take $g = 1$ and $z = pq$. We then have $G(d,e,k) = C_n$. When $d \neq 1$, all terms in (3) vanish unless $d = q$, $g = p$, when the term for $f = p$ gives $\varphi(q)^{-1}(q^1 - 1) = 1$. Thus (3) tells us that there is just one isomorphism type of nonabelian group of order n. Hence Proposition 3.6 does indeed give the correct number of isomorphism types for each factorisation. By similar reasoning (which we leave to the reader), Hölder's formula (1) correctly predicts two isomorphism classes of groups of order n.

We now turn to Theorem 2. The product over $p \mid d$ vanishes unless $d = 1$ or $d = q$, $g = p$. The nonzero contributions to (2) for the various factorisations $n = gzd$ are shown in Table 1. Summing the final column of Table 1 gives the correct count of $2(q-1)+1$ Hopf-Galois structures on a cyclic extension of degree $n = pq$. Table 1 also illustrates an important feature of the formula (2): factorisations

$n = dgz$ for which there are no corresponding groups G can nevertheless contribute nonzero terms to (2).

7.4. **Three Primes.** Let $n = p_1p_2p_3$ where $p_1 < p_2 < p_3$ are primes. Both the number of isomorphism classes of groups of order n, and the number of Hopf-Galois structures on a cyclic extension of degree n, depend on congruence conditions relating the three primes. There are two combinations of these conditions for which the Hopf-Galois structures on all Galois extensions of degree $p_1p_2p_3$ (not just cyclic extensions) have been enumerated.

The first of these is when $p_1 = 2$ and $p_3 = 2p_2 + 1$ (so p_2 is a Sophie Germain prime and p_3 is a safeprime). Kohl [Koh13, Theorem 5.1] treated this case as an application of his method for studying Hopf-Galois structures on Galois extensions of degree mp (with p prime and $m < p$). Those extensions with Galois group $\mathrm{Hol}(C_{p_3}) = C_{p_3} \rtimes C_{p_3-1}$ had previously been considered in [Chi03].

The second situation where all Hopf-Galois structures have been determined is when $p_1 > 2$ and $p_2 \equiv p_3 \equiv 1 \pmod{p_1}$ but $p_3 \not\equiv 1 \pmod{p_2}$. This case is treated in [Koh16, Theorem 2.4]. The same techniques could be applied to other combinations of congruence conditions, but separate calculations would be required for each case.

In the following, we will apply Theorem 1 to count the Hopf-Galois structures only on a *cyclic* extension of degree $n = p_1p_2p_3$, but under all possible combinations of congruence conditions. In particular, this will recover those parts of Kohl's results in [Koh13, Koh16] which relate to cyclic extensions.

In Table 2 we show the factorisations $n = dgz$ for which groups exist, the number of isomorphism types of these groups, and the number of Hopf-Galois structures of each isomorphism type.

The first column of Table 2 numbers the factorisations for ease of reference, and the factorisation is shown in the next 3 columns. The 5th column shows the congruence conditions which must be satisfied for groups to exist. The 6th column shows the number of isomorphism types of group corresponding to the given factorisation, as given by Proposition 3.6. These can also be found directly, as explained below. The final column shows the number of Hopf-Galois structures for each isomorphism type. This is given by the formula $2^{\omega(g)}\varphi(d)$ of Theorem 1.

We now explain how to find the values in the 6th column of Table 2 directly. (This illustrates in simple cases the proof of Proposition 3.6.) Consider for example case 2, where $d = p_1$, $g = p_2$, $z = p_3$, so $e = p_2p_3$. The distinct isomorphism types of groups $G(d, e, k)$ with

Case	d	g	z	Condition	# groups	# HGS per group
1	1	1	$p_1p_2p_3$		1	1
2	p_1	p_2	p_3	$p_2 \equiv 1 \pmod{p_1}$	1	$2(p_1-1)$
3	p_1	p_3	p_2	$p_3 \equiv 1 \pmod{p_1}$	1	$2(p_1-1)$
4	p_1	p_2p_3	1	$p_2 \equiv p_3 \equiv 1 \pmod{p_1}$	p_1-1	$4(p_1-1)$
5	p_2	p_3	p_1	$p_3 \equiv 1 \pmod{p_2}$	1	$2(p_2-1)$
6	p_1p_2	p_3	1	$p_3 \equiv 1 \pmod{p_1p_2}$	1	$2(p_1-1)(p_2-1)$

TABLE 2. Numbers of isomorphism types and Hopf-Galois structures for $n = p_1p_2p_3$.

these parameters correspond to subgroups $\langle k\rangle \subseteq U(p_2p_3)$ of order p_1 for which $z = \gcd(k-1, p_2p_3) = p_3$. Since $k \equiv 1 \pmod{p_3}$, we can identify $\langle k\rangle$ with a subgroup of order p_1 in $U(p_2)$. Such a subgroup exists since $p_2 \equiv 1 \pmod{p_1}$, and it is unique since $U(p_2)$ is cyclic. Thus there is just one group $G(d,e,k)$ in case 2. In case 4, however, where $d = p_1$, $g = p_2p_3$ and $z = 1$, the isomorphism types of groups $G(d,e,k)$ correspond to subgroups $\langle k\rangle \subseteq U(p_2p_3)$ of order p_1 with $\gcd(k-1, p_2p_3) = 1$. Now $U(p_2p_3) \cong U(p_2) \times U(p_3)$ contains p_1+1 subgroups of order p_1. For one of these, $\gcd(k-1, p_2p_3) = p_3$. This gives the group G just found in case 2. Another of the subgroups has $\gcd(k-1, p_2p_3) = p_2$, and this is counted in case 3. The remaining $p_1 - 1$ subgroups of $U(p_2p_3)$ give groups G with $g = p_2p_3$ and $z = 1$. Thus the number of groups recorded in case 4 is $p_1 - 1$.

We now find the total number of Hopf-Galois structures on a cyclic extension of degree n, treating each combination of relevant congruence conditions on p_1, p_2, p_3 separately. The results are shown in Table 3. For each combination of congruence conditions, we pick out the cases from Table 2 where any groups $G(d,e,k)$ exist. To obtain the total number of isomorphism types of groups of order n, we add the numbers of groups from the corresponding rows in Table 2, giving the entries in the 5th column of Table 3. These agree with the values given by Kohl [Koh16, p. 46]. To obtain the total number of Hopf-Galois structures, we multiply the entries in the final two columns of Table 2 and add these values for the appropriate rows. After simplification, this gives the entries in the final column of Table 3.

We now specialise to the two situations considered in [Koh13, Theorem 5.1] and [Koh16, Theorem 2.4] in order to confirm that we recover those parts of Kohl's results pertaining to cyclic extensions.

First let $p_1 = 2$ and let $p_3 = 2p_2 + 1$ be a safeprime. Thus we have $p_j \equiv 1 \pmod{p_i}$ whenever $1 \le i \le j \le 3$, corresponding to the

$p_2 \mid (p_3-1)$	$p_1 \mid (p_3-1)$	$p_1 \mid (p_2-1)$	Cases	# groups	Total # HGS
no	no	no	1	1	1
no	no	yes	1, 2	2	$2p_1-1$
no	yes	no	1, 3	2	$2p_1-1$
no	yes	yes	1, 2, 3, 4	p_1+2	$(2p_1-1)^2$
yes	no	no	1, 5	2	$2p_2-1$
yes	no	yes	1, 2, 5	3	$2p_1+2p_2-3$
yes	yes	no	1, 3, 5, 6	4	$2p_1p_2-1$
yes	yes	yes	1, 2, 3, 4, 5, 6	p_1+4	$4p_1^2+2p_1p_2-6p_1+1$

TABLE 3. Total numbers of Hopf-Galois structures for $n = p_1p_2p_3$.

final row ("yes–yes–yes") in our Table 3. The first row of the table in [Koh13, Theorem 5.1] shows that there are 6 isomorphism types of groups of order $n = p_1p_2p_3$, which Kohl denotes by C_{mp}, $C_p \times D_q$, $F \times C_2$, $C_q \times D_p$, D_{pq}, $\mathrm{Hol}(C_p)$, where $q = p_2$ and $p = p_3$. These contribute 1, 2, $2(p_2-1)$, 2, 4, $2(p_2-1)$ Hopf-Galois structures respectively. The total number of Hopf-Galois structures is therefore $4p_2+5$. These groups are respectively those of cases 1, 2, 5, 3, 4, 6 in our Table 2. Putting $p_1 = 2$ in Table 2, we again get $4p_2+5$ for the total number of Hopf-Galois structures, and the number of Hopf-Galois structures of each type shown in Table 2 agrees with Kohl's values. Thus our results recover the part of Kohl's result [Koh13, Theorem 5.1] relating to cyclic extensions of degree $2pq = 2p_2(2p_2+1)$.

Now let $p_1 > 2$ and $p_2 \equiv p_3 \equiv 1 \pmod{p_1}$ but $p_3 \not\equiv 1 \pmod{p_2}$, corresponding to the 4th row ("no–yes–yes") of our Table 3. The first row of the table in [Koh16, Theorem 2.4] shows that there are p_1+2 groups G. (Note that the final column, headed $C_{p_3p_2} \rtimes_i C_{p_1}$, corresponds to p_1-1 distinct isomorphism types, given by $1 \le i \le p_1-1$.) Of these groups, one contributes one Hopf-Galois structure, two contribute $2(p_1-1)$, and the rest $4(p_1-1)$. Thus there are in total of $(2p_1-1)^2$ Hopf-Galois structures. This agrees with our count in Table 3 and the relevant cases, 1–4, in Table 2. (The restriction $p_1 > 2$ turns out to be irrelevant when the Galois group is cyclic.)

7.5. **Four primes.** As a final example, we consider the case when $n = p_1p_2p_3p_4$ is the product of 4 distinct primes, under the assumption that

$$p_j \equiv 1 \pmod{p_i} \text{ whenever } i < j. \tag{16}$$

d	g	z	# groups	# HGS per group
1	1	$p_1p_2p_3p_4$	1	1
p_1	p_2	p_3p_4	1	$2(p_1-1)$
p_1	p_3	p_2p_4	1	$2(p_1-1)$
p_1	p_4	p_2p_3	1	$2(p_1-1)$
p_1	p_2p_3	p_4	p_1-1	$4(p_1-1)$
p_1	p_2p_4	p_3	p_1-1	$4(p_1-1)$
p_1	p_3p_4	p_2	p_1-1	$4(p_1-1)$
p_1	$p_2p_3p_4$	1	$(p_1-1)^2$	$8(p_1-1)$
p_2	p_3	p_1p_4	1	$2(p_2-1)$
p_2	p_4	p_1p_3	1	$2(p_2-1)$
p_2	p_3p_4	p_1	p_2-1	$4(p_2-1)$
p_3	p_4	p_1p_2	1	$2(p_3-1)$
p_1p_2	p_3	p_4	1	$2(p_1-1)(p_2-1)$
p_1p_2	p_4	p_3	1	$2(p_1-1)(p_2-1)$
p_1p_2	p_3p_4	1	$(p_1+1)(p_2+1)-2$	$4(p_1-1)(p_2-1)$
p_1p_3	p_4	p_2	1	$2(p_1-1)(p_3-1)$
p_2p_3	p_4	p_1	1	$2(p_2-1)(p_3-1)$
$p_1p_2p_3$	p_4	1	1	$2(p_1-1)(p_2-1)(p_3-1)$

Table 4. Numbers of isomorphism types and Hopf-Galois structures for $n = p_1p_2p_3p_4$.

(Thus we have $p_1 < p_2 < p_3 < p_4$.)

We record in Table 4 the number of isomorphism classes of groups $G(d, e, k)$, and the number of Hopf-Galois structures of each type, corresponding to each relevant factorisation $n = dgz$.

It follows from this table that, under the assumption (16), there are $p_1^2 + p_1p_2 + 2p_1 + 2p_2 + 8$ isomorphism types of groups of order $n = p_1p_2p_3p_4$, and the total number of Hopf-Galois structures is

$$4p_1^2p_2^2 + 8p_1^3 + 2p_1p_2p_3 - 16p_1^2 - 6p_1p_2 + 10p_1 - 1.$$

For example, if $n = 2\cdot3\cdot7\cdot43 = 1806$, or more generally, if $n = 42p_4$ for any prime $p_4 \equiv 1 \pmod{42}$, then a cyclic extension of degree n admits precisely 211 Hopf-Galois structures of 28 different types.

When (16) does not hold, we can enumerate the Hopf-Galois structures by picking out the appropriate rows in Table 4, just as we did in §7.4.

References

[BC12] Nigel P. Byott and Lindsay N. Childs, *Fixed-point free pairs of homomorphisms and nonabelian Hopf-Galois structures*, New York J. Math. **18** (2012), 707–731. MR 2991421

[Byo96] Nigel P. Byott, *Uniqueness of Hopf Galois structure for separable field extensions*, Comm. Algebra **24** (1996), no. 10, 3217–3228. MR 1402555

[Byo04a] ———, *Hopf-Galois structures on field extensions with simple Galois groups*, Bull. London Math. Soc. **36** (2004), no. 1, 23–29. MR 2011974

[Byo04b] ———, *Hopf-Galois structures on Galois field extensions of degree pq*, J. Pure Appl. Algebra **188** (2004), no. 1-3, 45–57. MR 2030805

[Byo13] ———, *Nilpotent and abelian Hopf-Galois structures on field extensions*, J. Algebra **381** (2013), 131–139. MR 3030514

[Byo15] ———, *Solubility criteria for Hopf-Galois structures*, New York J. Math. **21** (2015), 883–903. MR 3425626

[Chi89] Lindsay N. Childs, *On the Hopf Galois theory for separable field extensions*, Comm. Algebra **17** (1989), no. 4, 809–825. MR 990979

[Chi00] ———, *Taming wild extensions: Hopf algebras and local Galois module theory*, Mathematical Surveys and Monographs, vol. 80, American Mathematical Society, Providence, RI, 2000. MR 1767499

[Chi03] ———, *On Hopf Galois structures and complete groups*, New York J. Math. **9** (2003), 99–115. MR 2016184

[Chi05] ———, *Elementary abelian Hopf Galois structures and polynomial formal groups*, J. Algebra **283** (2005), no. 1, 292–316. MR 2102084

[CRV16] Teresa Crespo, Anna Rio, and Montserrat Vela, *Induced Hopf Galois structures*, J. Algebra **457** (2016), 312–322. MR 3490084

[GP87] Cornelius Greither and Bodo Pareigis, *Hopf Galois theory for separable field extensions*, J. Algebra **106** (1987), no. 1, 239–258. MR 878476

[Höl95] Otto Hölder, *Die Gruppen mit quatratfreier Ordnungszahl*, Nachr. Königl. Ges. Wiss. Göttingen Math. Phys. **1** (1895), 211–229.

[Koh98] Timothy Kohl, *Classification of the Hopf Galois structures on prime power radical extensions*, J. Algebra **207** (1998), no. 2, 525–546. MR 1644203

[Koh13] ———, *Regular permutation groups of order mp and Hopf Galois structures*, Algebra Number Theory **7** (2013), no. 9, 2203–2240. MR 3152012

[Koh16] ———, *Hopf-Galois structures arising from groups with unique subgroup of order p*, Algebra Number Theory **10** (2016), no. 1, 37–59. MR 3463035

[MM84] M. Ram Murty and V. Kumar Murty, *On groups of squarefree order*, Math. Ann. **267** (1984), no. 3, 299–309. MR 738255

[Rob96] Derek J. S. Robinson, *A course in the theory of groups*, second ed., Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York, 1996. MR 1357169

(A. Alabdali) Department of Mathematics, College of Engineering, Mathematics and Physical Sciences, University of Exeter, Exeter EX4 4QF U.K.

(A. Alabdali) Department of Mathematics, College of Education for Pure Science, University of Mosul, Mosul, Iraq.
E-mail address: aaab201@exeter.ac.uk

(N. Byott) Department of Mathematics, College of Engineering, Mathematics and Physical Sciences, University of Exeter, Exeter EX4 4QF U.K.
E-mail address: N.P.Byott@exeter.ac.uk