New York Journal of Mathematics

New York J. Math. **21** (2015) 883–903.

Solubility criteria for Hopf–Galois structures

Nigel P. Byott

Abstract. Let L/K be a finite Galois extension of fields with group Γ. Associated to each Hopf–Galois structure on L/K is a group G of the same order as the Galois group Γ. The *type* of the Hopf–Galois structure is by definition the isomorphism type of G. We investigate the extent to which general properties of either of the groups Γ and G constrain those of the other. Specifically, we show that if G is nilpotent then Γ is soluble, and that if Γ is abelian then G is soluble. In contrast to these results, we give some examples where the groups Γ and G have different composition factors. In particular, we show that a soluble extension may admit a Hopf–Galois structure of insoluble type.

Contents

1. Introduction and statement of results

Hopf–Galois theory was initiated by Chase and Sweedler [CS69], motivated in part by a wish to develop a version of Galois theory for inseparable field extensions. Their approach nevertheless gives an interesting perspective on the classical theory for separable extensions. The problem of finding all Hopf–Galois structures on a given separable extension L/K was expressed in terms of group theory by Greither and Pareigis [GP87], who showed that L may admit H-Galois structures for a number of different K-Hopf algebras H. Moreover, it can happen that the same Hopf algebra H may have

Received August 26, 2015.
2010 *Mathematics Subject Classification.* 12F10, 16T05, 20D05.
Key words and phrases. Hopf–Galois structure; soluble group; simple group.

ISSN 1076-9803/2015

several different actions on L, giving rise to different Hopf–Galois structures [CCo07, CRV15].

In the special case that L/K is a Galois extension (i.e., normal as well as separable) with group $\Gamma = \mathrm{Gal}(L/K)$, the main result of [GP87] is that the Hopf–Galois structures on L/K correspond to regular subgroups G of the group $\mathrm{Perm}(\Gamma)$ of permutations of Γ such that G is normalized by left translations by Γ. The groups Γ and G necessarily have the same order, but in general need not be isomorphic. We refer to the isomorphism type of G as the *type* of the Hopf–Galois structure.

A number of authors have used the framework developed in [GP87] to investigate Hopf–Galois structures on various classes of separable extensions. Apart from their intrinsic interest, one motivation for studying multiple Hopf–Galois structures on the same extension is their relevance to questions of integral Galois module structure: the ring of integers in a Galois extension of local fields may have better module-theoretic properties in one of the nonclassical Hopf–Galois structures than it does in the classical Galois structure [Byo97].

A considerable amount is now known about Hopf–Galois structures on Galois extensions L/K. For an odd prime p, a cyclic extension of degree p^n admits precisely p^{n-1} Hopf–Galois structures, all of cyclic type [Koh98], while an elementary abelian extension of degree p^n admits at least $p^{n(n-1)-1}(p-1)$ Hopf–Galois structures of elementary abelian type if $p > n$ [Chi05]. If p and q are distinct primes such that there exists a nonabelian group of order pq, then any Galois extension of degree pq, whether abelian or not, admits Hopf–Galois structures both of abelian type and of nonabelian type [Byo04a]. More generally, Galois extensions of degree mp, with p prime and $m < p$, are considered in [Koh13]. In contrast to the cyclic prime-power case, "most" abelian extensions admit Hopf–Galois structures of nonabelian type [BC12]. A Galois extension whose group Γ is a nonabelian simple group admits precisely two Hopf–Galois structures, both of type Γ [Byo04b], whereas an extension with symmetric Galois group S_n admits many Hopf–Galois structures of type S_n and also many of type $A_n \times C_2$ [CaC99].

There are fewer results relating to the more general situation where L/K is separable but not necessarily normal. A separable extension of prime degree is Hopf–Galois if and only if its Galois closure has soluble Galois group [Chi89]. For an odd prime p, the Hopf–Galois structures on a radical extension $K(\sqrt[p^n]{a})/K$ of degree p^n are enumerated in [Koh98], the result depending on which roots of unity occur in K. The corresponding result for $p = 2$ is given in [Byo07]. The Hopf–Galois characters of all separable extensions L/K of degree ≤ 6 have recently been determined [CRVa], together with those of the extensions F/K with $L \subset F \subset N$, where N is the normal closure of L/K.

For a more extensive review of results in separable Hopf–Galois theory, we refer the reader to [CRVb].

In this paper, we consider only Galois extensions. Let L/K be a Galois extension with Galois group Γ, and suppose that L/K admits a Hopf–Galois structure of type G. We investigate the extent to which group-theoretic properties of either one of the groups Γ or G constrain the other. Already in the case of groups of order pq mentioned above, it may happen that either one of the groups is abelian while the other is not, and indeed is not even nilpotent. This shows, for example, that it is possible for an extension of finite fields to admit a Hopf–Galois structure which is not of nilpotent type. Our two main results will give criteria, in terms of each of the groups Γ and G, for the other to be soluble:

Theorem 1. *With the above notation, if G is nilpotent then Γ is soluble. Thus, if a finite Galois extension of fields admits a Hopf–Galois structure of nilpotent type, then the extension has soluble Galois group.*

Theorem 2. *If Γ is abelian then G is soluble. Thus, any Hopf–Galois structure on a finite abelian field extension has soluble type.*

Theorem 1 is an application of the theory of Hall p'-subgroups.

We shall in fact give two proofs of Theorem 2. The first builds on the methods of [Byo04b] and depends on the classification of finite simple groups. In particular, it uses a result of Vdovin [Vdo99] which bounds the size of abelian subgroups in a nonabelian simple group. The author is grateful to the referee of an earlier version of this paper for drawing his attention to the work of Li [Li03], by means of which a much shorter and more direct proof of Theorem 2 can be given and the use of the classification avoided. Li classifies the finite primitive permutation groups which contain an abelian regular subgroup, thereby solving a problem which goes back to Burnside. This depends heavily on the classification of finite simple groups, but (without using the classification) Li proves as a preliminary result [Li03, Lemma 3.2] that a transitive permutation group with an insoluble regular normal subgroup cannot contain an abelian regular subgroup. Our second proof of Theorem 2 is an easy deduction from this. Despite the greater length and complexity of the first proof, we believe that the ideas which underlie it give insights that may be valuable for future work on Hopf–Galois structures, as explained in Remark 6.3 below. We have therefore decided to present both proofs in this paper.

In the situations of Theorems 1 and 2, Γ and G are soluble groups of the same order, so certainly have the same composition factors. In the various results for Galois extensions L/K mentioned above, it is again clear that the composition factors of Γ and G coincide. It is therefore natural to ask whether, in general, the existence of a Hopf–Galois structure of type G on a Galois extension with group Γ necessarily forces Γ and G to have the same composition factors. We will answer this question in the negative by proving the following result:

Theorem 3. *Let G be a finite nonabelian simple group containing a subgroup H of prime-power index, $|G : H| = p^a$ for p prime and $a \geq 1$. Then there exists a subgroup J of G of order p^a such that any Galois extension of fields with Galois group $\Gamma = H \times J$ admits a Hopf–Galois structure of type G.*

The proof of Theorem 3 uses Guralnick's determination [Gur83] of the nonabelian simple groups with a subgroup of prime-power index (which depends on the classification of finite simple groups, and is recalled as Theorem 6 in §7 below). This is combined with the method of constructing Hopf–Galois structures via fixed-point free pairs of homomorphism, introduced in [CCo07] in the case $G = \Gamma$ and extended to the case $G \neq \Gamma$ in [BC12].

In particular, there exist finite soluble groups Γ such that every Galois extension with group Γ admits a Hopf–Galois structure of insoluble type. We collect together some examples of this phenomenon in Corollary 1.1 below, where we use the following notation. As usual, C_n, S_n, A_n and D_{2n} denote respectively the cyclic group of order n, the symmetric and alternating groups of degree n, and the dihedral group of order $2n$. For a prime p, we write $\mathrm{PSL}_m(p)$ for the projective special linear group of dimension m over the field $\mathbb{F}_p$ of p elements. When p is odd, we also write $F_{\frac{1}{2}p(p-1)}$ for the unique Frobenius group of order $\frac{1}{2}p(p-1)$ that has a faithful permutation representation of degree p, namely the semidirect product $C_p \rtimes C_{\frac{1}{2}(p-1)}$ in which the second factor acts faithfully on the first.

Corollary 1.1.

(i) *Any Galois extension of degree* 60 *with* (*soluble*) *Galois group*
$$\Gamma = A_4 \times C_5$$
admits a Hopf–Galois structure of (*simple*) *type* A_5.

(ii) *Any Galois extension of degree* 168 *with* (*soluble*) *Galois group*
$$\Gamma = S_4 \times C_7$$
admits a Hopf–Galois structure of (*simple*) *type* $\mathrm{PSL}_3(2) \cong \mathrm{PSL}_2(7)$.

(iii) *If $p = 2^e - 1 \geq 7$ is a Mersenne prime, then any Galois extension of degree $\frac{1}{2}(p-1)p(p+1)$ with* (*soluble*) *Galois group $\Gamma = F_{\frac{1}{2}p(p-1)} \times D_{2^e}$ admits a Hopf–Galois structure of* (*simple*) *type* $\mathrm{PSL}_2(p)$.

We do not have any examples where an extension with insoluble Galois group Γ admits a Hopf–Galois structure of soluble type G.

2. Preliminaries on Hopf–Galois structures

Let L/K be a field extension of finite degree n, and let H be a K-Hopf algebra with comultiplication $\Delta\colon H \longrightarrow H \otimes_K H$, $\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)}$, and augmentation (counit) $\epsilon\colon H \longrightarrow K$. We say that L is an H-module algebra if H acts on L so that $h\cdot(xy) = \sum_{(h)}(h_{(1)}\cdot x)(h_{(2)}\cdot y)$ and $h\cdot k = \epsilon(h)k$

for all $h \in H$, x, $y \in L$ and $k \in K$. We say that L is an H-Galois extension of K if, furthermore, the K-linear map $\theta\colon L \otimes_K L \longrightarrow \mathrm{Hom}_K(H, L)$, given by $\theta(x \otimes y)(h) = x(h \cdot y)$ for x, $y \in L$ and $h \in H$, is bijective. We then also say that H endows L with a Hopf–Galois structure.

When L/K is separable, Greither and Pareigis [GP87] gave the following characterization of the Hopf–Galois structures on L/K. Let E be the normal closure of L/K and consider the Galois groups $\Gamma = \mathrm{Gal}(E/K)$ and $\Gamma' = \mathrm{Gal}(E/L)$. Let Γ/Γ' denote the set of left cosets $\gamma\Gamma'$ of Γ' in Γ, and let $\mathrm{Perm}(\Gamma/\Gamma')$ be the group of permutations of this set. Thus $\mathrm{Perm}(\Gamma/\Gamma')$ is isomorphic to the symmetric group S_n. The left translations by elements of Γ form a subgroup $\lambda(\Gamma)$ of $\mathrm{Perm}(\Gamma/\Gamma')$, which we identify with Γ. The Hopf–Galois structures on L/K, up to isomorphism, correspond bijectively with regular subgroups G of $\mathrm{Perm}(\Gamma/\Gamma')$ which are normalized by $\lambda(\Gamma)$. (A permutation group acting on a set X is said to be regular if it is transitive and the stabilizer of any element of X is the identity.) In the Hopf–Galois structure corresponding to such a subgroup G, the Hopf algebra acting on L is $E[G]^\Gamma$, the fixed point algebra of the group algebra $E[G]$ under the action of Γ simultaneously on E by field automorphisms and on G by conjugation by left translations inside $\mathrm{Perm}(\Gamma/\Gamma')$. We refer to the isomorphism type of G as the *type* of the Hopf–Galois structure.

If L/K is also normal, which will always be the case in this paper, then $E = L$, Γ' is trivial, and $\Gamma = \mathrm{Gal}(L/K)$. The result of Greither and Pareigis then simplifies to the statement given in the introduction. In particular, Γ and G are finite groups of the same order n. Moreover, if Γ normalizes G in $\mathrm{Perm}(\Gamma)$ then we can view Γ as being contained in the holomorph $\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G)$ of G, which is usually a much smaller group than $\mathrm{Perm}(\Gamma)$. Thus, given an abstract group G of the same order as Γ, there exists a Hopf–Galois structure on L/K of type G if and only if there is an embedding $\beta\colon \Gamma \longrightarrow \mathrm{Hol}(G)$ with regular image. We shall call such a β a regular embedding. Then the number of Hopf–Galois structures of type G is the number of equivalence classes of regular embeddings, where two embeddings are equivalent if and only if they are conjugate in $\mathrm{Hol}(G)$ by an element of $\mathrm{Aut}(G)$; see [Byo96] or [Chi00, §7].

It is convenient to write elements of $\mathrm{Hol}(G)$ in the form $[g, \alpha]$ with $g \in G$ and $\alpha \in \mathrm{Aut}(G)$. The multiplication in $\mathrm{Hol}(G)$ is then given by

$$[g_1, \alpha_1][g_2, \alpha_2] = [g_1\alpha_1(g_2), \alpha_1\alpha_2]. \tag{1}$$

3. Nilpotent Hopf–Galois structures

In this section, we prove Theorem 1. Thus we suppose that L/K is a finite Galois extension of fields with group $\mathrm{Gal}(L/K) = \Gamma$, and that L/K admits a Hopf–Galois structure of type G for some nilpotent group G. We then have a regular embedding $\beta : \Gamma \longrightarrow \mathrm{Hol}(G)$. Moreover, being nilpotent, G

can be written as the direct product

$$G = \prod_p G_p$$

over all primes p, where G_p denotes the (unique) Sylow p-subgroup of G [Rob96, 5.2.4]. Our task is to show that the group Γ is soluble.

If J is a finite group of order $p^r m$, where p is prime and $p \nmid m$, then a subgroup of J of order m is called a Hall p'-subgroup of J. We will use P. Hall's theorem [Rob96, 9.1.8] that if J has a Hall p'-subgroup for every prime p, then J is soluble.

For each p, let

$$H_p = \prod_{q \neq p} G_q.$$

Then H_p is a Hall p'-subgroup of G. Moreover, H_p is a characteristic subgroup of G, as it consists precisely of the elements of order prime to p.

Define $\Delta_p = \{\gamma \in \Gamma \ : \ \beta(\gamma) \cdot e_G \in H_p\}$, where e_G is the identity element of G. Since $\beta(\Gamma)$ is regular on G, it is clear that Δ_p is a *subset* of Γ of size $|H_p|$. However, since H_p is characteristic in G, more is true:

Lemma 3.1. *Δ_p is a subgroup of Γ.*

Proof. As Δ_p is nonempty and Γ is finite, it suffices to check that Δ_p is closed under multiplication. So let σ_1, $\sigma_2 \in \Delta_p$, and let $h_i = \beta(\sigma_i) \cdot e_G$ for $i = 1, 2$. Thus $h_i \in H_p$, and, in the notation of (1), we have $\beta(\sigma_i) = [h_i, \alpha_i]$ for some $\alpha_i \in \mathrm{Aut}(G)$. Then $\beta(\sigma_1\sigma_2) = [h_1\alpha_1(h_2), \alpha_1\alpha_2]$, so that $\beta(\sigma_1\sigma_2) \cdot e_G = h_1\alpha(h_2)$. Since H_p is a characteristic subgroup of G, we have $\alpha_1(h_2) \in H_p$ and hence $\beta(\sigma_1\sigma_2) \cdot e_G \in H_p$. Thus $\sigma_1\sigma_2 \in \Delta_p$, as required. □

As $|\Gamma| = |G|$ and $|\Delta_p| = |H_p|$, it follows that Δ_p is a Hall p'-subgroup of Γ. Thus Γ contains a Hall p'-subgroup Δ_p for each prime p. Hence, by Hall's theorem, Γ is soluble. This completes the proof of Theorem 1.

4. First proof of Theorem 2

In this section and the next, we give our first proof of Theorem 2, which depends on the classification of finite simple groups. In this section, we reduce the proof of Theorem 2 to that of a statement, Theorem 4, about simple groups. Theorem 4 will then be proved in §5 using Vdovin's theorem [Vdo99] (Theorem 5 in §5 below).

Before stating Theorem 4, we introduce some notation.

Definition 4.1. Let G be a finite group. Then

$$a(G) = \max\{\ |A| \ : \ A \text{ is an abelian subgroup of } G\}.$$

We note another result from Vdovin's paper, and record some obvious properties of $a(G)$.

Proposition 4.2. *For the symmetric group S_m, we have $a(S_m) \leq 3^{m/3}$.*

Proof. From [Vdo99, Theorem 1.1], we have $a(S_{3k}) = 3^k$, $a(S_{3k+1}) = 4 \cdot 3^{k-1}$ and $a(S_{3k+2}) = 2 \cdot 3^k$. Hence the stated inequality holds in all cases. □

Proposition 4.3. *Let G be a finite group.*

(i) *If H is a subgroup of G then $a(H) \leq a(G)$.*
(ii) *If N is a normal subgroup of G then $a(G) \leq a(N)a(G/N)$.*
(iii) *If $G = H \times J$ then $a(G) = a(H)a(J)$. In particular*

$$a(H^m) = a(H)^m.$$

Proof. (i) Any abelian subgroup of H is certainly an abelian subgroup of G.

(ii) Let A be an abelian subgroup of G, and let A_1 (respectively, A_2) be the kernel (respectively, image) of the composite homomorphism

$$A \hookrightarrow G \twoheadrightarrow G/N.$$

Then $|A| = |A_1|\,|A_2| \leq a(N)a(G/N)$.

(iii) Let $G = H \times J$. By (ii), $a(G) \leq a(H)a(J)$. But if $A \subseteq H$, $B \subseteq J$ are abelian subgroups with $|A| = a(H)$, $|B| = a(J)$, then $A \times B$ is an abelian subgroup of G of order $a(H)a(J)$. This gives the first assertion, and the second follows by induction. □

We will deduce Theorem 2 from the following statement:

Theorem 4. *Let T be a finite nonabelian simple group. Then*

$$3^{1/3}a(T)a(\mathrm{Aut}(T)) < |T|. \tag{2}$$

Proof of Theorem 2 (assuming Theorem 4). Let Γ be a finite abelian group. We need to show that if there is a regular embedding $\beta\colon \Gamma \longrightarrow \mathrm{Hol}(G)$ for some group G, then G must be soluble.

We first treat the special case where G is characteristically simple. Thus, by [Rob96, 3.3.15], G is the direct product T^m for some simple group T and some $m \geq 1$. We claim that the existence of a regular embedding $\Gamma \longrightarrow \mathrm{Hol}(T^m)$, with Γ abelian, forces T to be abelian. Then G is abelian, and hence soluble, as required.

Suppose that T is a nonabelian simple group. Then, by [Byo04b, Lemma 3.2], $\mathrm{Aut}(T^m)$ is the wreath product

$$\mathrm{Aut}(T^m) = \mathrm{Aut}(T) \wr S_m = (\mathrm{Aut}(T)^m) \rtimes S_m,$$

where the symmetric group S_m permutes the m factors. We therefore have a regular embedding of the abelian group Γ in

$$\mathrm{Hol}(T^m) = T^m \rtimes (\mathrm{Aut}(T)^m \rtimes S_m).$$

We break $\mathrm{Hol}(T^m)$ into the sequence of quotients

$$H_1 = \frac{\mathrm{Hol}(T^m)}{\mathrm{Hol}(T)^m} \cong \frac{T^m \rtimes (\mathrm{Aut}(T)^m \rtimes S_m)}{(T \rtimes \mathrm{Aut}(T))^m} \cong S_m,$$

$$H_2 = \frac{\mathrm{Hol}(T)^m}{T^m} \cong \mathrm{Aut}(T)^m;$$

$$H_3 = T^m.$$

As $|T|^m = |G| = |\Gamma| = |\beta(\Gamma)|$, we may apply Proposition 4.3(ii) twice to get $|T|^m \leq a(H_1)a(H_2)a(H_3)$. Now $a(H_1) \leq 3^{m/3}$ by Proposition 4.2, and $a(H_2) = a(\mathrm{Aut}(T)^m) = a(\mathrm{Aut}(T))^m$ and $a(H_3) = a(T)^m$ by Proposition 4.3(iii). Thus we have

$$|T|^m \leq 3^{m/3} a(\mathrm{Aut}(T))^m a(T)^m,$$

contradicting Theorem 4. Hence T is abelian, as claimed, and Theorem 2 holds when G is characteristically simple.

We now prove the general case by induction on $|G| = |\Gamma|$, taking the case just considered as the base of the induction. If G is not characteristically simple then it has a nontrivial proper characteristic subgroup H, and by [Byo04b, Proposition 3.1], β induces a homomorphism

$$\overline{\beta} : \Gamma \longrightarrow \mathrm{Hol}(G/H)$$

whose image is transitive on G/H. This image is also abelian, and is therefore regular on G/H. Let $\Sigma = \ker(\overline{\beta})$. Then $|\Sigma| = |H|$ and the abelian group Σ acts regularly on H, so β restricts to a regular embedding $\Sigma \longrightarrow \mathrm{Hol}(H)$. As $|H|, |G/H| < |G|$, it follows from the induction hypothesis that H and G/H are soluble, and hence so is G. □

5. Proof of Theorem 4

To complete the proof of Theorem 2, we must prove Theorem 4. We do so using the classification of finite simple groups. Our main reference for the necessary facts about the simple groups is the book [Wil09]. We also use [Gor82]. In brief, the classification states that every finite nonabelian simple group is either an alternating group A_n, $n \geq 5$, a (classical or exceptional) group of Lie type, or one of the 26 sporadic simple groups. We refer the reader to [Wil09, p. 3] for a more detailed statement.

Using the classification, Vdovin [Vdo99, Theorem A] proved the following result:

Theorem 5 (Vdovin)**.** *Let T be a finite nonabelian simple group which is not of the form* $\mathrm{PSL}_2(q)$*. Then $a(T)^3 < |T|$.*

Remark 5.1. Some of the groups $\mathrm{PSL}_2(q)$ appear in the classification in another guise, so that some families in the classification other than $\mathrm{PSL}_2(q)$ contain groups for which the conclusion of Vdovin's theorem does not hold. Thus, for the alternating group A_5 of order 60, we have $a(A_5) = 5 > 60^{1/3}$, but this does not contradict Vdovin's theorem since

$$A_5 \cong \mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5).$$

For any nonabelian simple group T, the group $\mathrm{Aut}(T)$ contains the subgroup $\mathrm{Inn}(T) \cong T$ of inner automorphisms, and we write

$$\mathrm{Out}(T) = \frac{\mathrm{Aut}(T)}{\mathrm{Inn}(T)}$$

for the group of outer automorphisms. Using Proposition 4.3(ii), we then have

$$a(\mathrm{Aut}(T)) \leq a(\mathrm{Inn}(T))a(\mathrm{Out}(T)) \leq a(T)|\mathrm{Out}(T)|. \tag{3}$$

A famous consequence of the classification is the proof of the Schreier Conjecture, which asserts that $\mathrm{Out}(T)$ is always soluble. Of greater relevance for us is the fact that $\mathrm{Out}(T)$ is very small relative to T. We will use this fact in conjunction with the following result.

Proposition 5.2. *Let T be a nonabelian simple group which is not of the form $\mathrm{PSL}_2(q)$. If the inequality*

$$3|\mathrm{Out}(T)|^3 < |T| \tag{4}$$

holds, then the conclusion (2) of Theorem 4 holds for T.

Proof. Since $a(T) < |T|^{1/3}$ by Theorem 5, it follows from (3) and (4) that

$$\begin{aligned} 3^{1/3}a(T)a(\mathrm{Aut}(T)) &\leq 3^{1/3}a(T)^2|\mathrm{Out}(T)| \\ &< a(T)^2|T|^{1/3} \\ &< |T|. \end{aligned}$$

□

Thus (2) holds.

By the classification of finite simple groups, together with Proposition 5.2, the proof of Theorem 4 is reduced to the following five lemmas, whose proofs will occupy the rest of this section.

Lemma 5.3. *The conclusion (2) of Theorem 4 holds for each alternating group $T = A_n$, $n \geq 5$.*

Lemma 5.4. *The inequality (4) of Proposition 5.2 holds for each sporadic simple group T.*

Lemma 5.5. *The conclusion (2) of Theorem 4 holds for each simple group T of the form $\mathrm{PSL}_2(q)$.*

Lemma 5.6. *The inequality (4) of Proposition 5.2 holds for each simple group T which is a classical group of Lie type but is not of the form $\mathrm{PSL}_2(q)$.*

Lemma 5.7. *The inequality (4) of Proposition 5.2 holds for each simple group T which is an exceptional group of Lie type.*

The first two cases are easily handled.

Proof of Lemma 5.3. We treat all the simple alternating groups $T = A_n$, $n \geq 5$ here, even though some of them are of the form $\mathrm{PSL}_2(q)$. In all cases, we have $a(A_n) \leq a(S_n) \leq 3^{n/3}$ by Propositions 4.3(i) and 4.2. For $T = A_n$ with $n \neq 6$, we have $|\mathrm{Out}(A_n)| = 2$ and $\mathrm{Aut}(A_n) \cong S_n$, whereas $|\mathrm{Out}(A_6)| = 4$ and $\mathrm{Aut}(A_6)$ has a normal subgroup of index 2 isomorphic to S_6 [Wil09, pp. 18, 19]. Thus for $n \neq 6$, we have $3^{1/3}a(T)a(\mathrm{Aut}(T) \leq 3^{(2n+1)/3}$ and (2) will hold provided that

$$3^{(2n+1)/3} < \tfrac{1}{2}n!.$$

But this inequality holds for $n = 5$ and hence, by induction, for all $n \geq 5$. In the exceptional case $T = A_6$, we have $a(\mathrm{Aut}(T))) \leq 2a(S_6) \leq 18$, so $3^{1/3}a(T)a(\mathrm{Aut}(T)) \leq 2 \cdot 3^{13/3} < 360 = |T|$, and again (2) holds. □

Proof of Lemma 5.4. Let T be a sporadic simple group. From [Gor82, p. 304], we have $|\mathrm{Out}(T)| \leq 2$. Thus $3|\mathrm{Out}(T)|^3 \leq 24 < |T|$, so (4) holds. □

Before giving the proofs of Lemmas 5.5–5.7, we recall some general properties of the finite simple groups of Lie type and their outer automorphisms, and we summarize the facts we will need about the various families of groups in Tables 1–4 below. The information in these tables is taken from [Wil09, Chapters 3, 4] and [Gor82, p. 135]. The outer automorphisms for most of the groups of Lie type are also described in [Ste60].

The groups in each family are indexed by a prime-power parameter q, and we will always write $q = p^e$ with p prime. Each simple group T of Lie type is obtained as the central quotient of some group of matrices over a finite field. Following [Gor82, p. 135], and changing notation from the previous sections, we denote this group by G, and we write d for the order of its center. We therefore have $|T| = |G|/d$. For example, if T is the projective special linear group $\mathrm{PSL}_n(q)$ then the corresponding group G is $\mathrm{SL}_n(q)$ whose center has order $d = (n, q-1)$. We list the classical simple groups T of Lie type in Table 1, together with the corresponding groups G and their orders. The value of d is shown in Table 2, along with the quantities ϵ and g which will be explained below. The exceptional simple Lie groups T, and the orders of the corresponding groups G, are given in Table 3, with the values of d, ϵ and g for each group shown in Table 4. We use the notation of [Wil09] for the groups T, but the notation of [Gor82] for the groups G. The notation for the groups G is derived from the standard labelling of the associated Dynkin diagrams. For example, the group $\mathrm{SL}_n(q)$ is denoted $A_{n-1}(q)$ as it corresponds to the Dynkin diagram A_{n-1}.

We have the generic isomorphism $\mathrm{P}\Omega_5(q) \cong \mathrm{PSp}_4(q)$ [Wil09, p. 96]. Following [Wil09], we omit the groups $\mathrm{P}\Omega_5(q)$ from the classification (whereas [Gor82] omits the groups $\mathrm{PSp}_4(q)$ instead). Also, $\mathrm{P}\Omega_{2n+1}(q) \cong \mathrm{PSp}_{2n}(q)$ when $q = 2^e$, so the groups $\mathrm{P}\Omega_{2n+1}(q)$ for q even could be omitted.

For each simple group T of Lie type, any outer automorphism of T may be written as a product of a diagonal automorphism, a field automorphism and a graph automorphism. The diagonal automorphisms arise from conjugation

T	restrictions	G	$\lvert G\rvert$
$\mathrm{PSL}_n(q)$	$n \geq 2$ $(n,q) \neq (2,2)$ $(n,q) \neq (2,3)$	$A_{n-1}(q)$	$q^{\frac{1}{2}n(n-1)} \prod_{i=2}^{n}(q^i - 1)$
$\mathrm{PSU}_n(q)$	$n \geq 3$ $(n,q) \neq (3,2)$	${}^2A_{n-1}(q)$	$q^{\frac{1}{2}n(n-1)} \prod_{i=2}^{n}(q^i - (-1)^i)$
$\mathrm{PSp}_{2n}(q)$	$n \geq 2$ $(n,q) \neq (2,2)$	$C_n(q)$	$q^{n^2} \prod_{i=1}^{n}(q^{2i} - 1)$
$\mathrm{P\Omega}_{2n+1}(q)$	$n \geq 3$	$B_n(q)$	$q^{n^2} \prod_{i=1}^{n}(q^{2i} - 1)$
$\mathrm{P\Omega}^+_{2n}(q)$	$n \geq 4$	$D_n(q)$	$q^{n(n-1)}(q^n - 1)\prod_{i=1}^{n-1}(q^{2i} - 1)$
$\mathrm{P\Omega}^-_{2n}(q)$	$n \geq 4$	${}^2D_n(q)$	$q^{n(n-1)}(q^n + 1)\prod_{i=1}^{n-1}(q^{2i} - 1)$

TABLE 1. Classical simple groups of Lie type

of G by elements of a larger matrix group in which G is normal. For example, the diagonal automorphisms of $\mathrm{PSL}_n(q)$ are induced by the automorphisms of $\mathrm{SL}_n(q)$ arising from conjugation by elements of $\mathrm{GL}_n(q)$. In all cases, the number of such diagonal automorphisms is the quantity d described above. The field automorphisms are induced by automorphisms of the underlying finite field, and therefore form a cyclic group. We write ϵ for the number of field automorphisms. In most cases, $\epsilon = e$ as we are working with matrices over the field $\mathbb{F}_q$ of $q = p^e$ elements. The exceptions are that $\epsilon = 2e$ for the families $\mathrm{PSU}_n(q)$, $\mathrm{P\Omega}^-_{2n}(q)$ and ${}^2E_6(q)$, since these groups are obtained from groups of matrices over $\mathbb{F}_{q^2}$, and $\epsilon = 3e$ for ${}^3D_6(q)$ where the matrices are over $\mathbb{F}_{q^3}$. Finally, the graph automorphisms arise from automorphisms of the Dynkin diagram where, for groups in characteristic p, the automorphism does not need to preserve the direction of the arrow on an edge of multiplicity p. We write g for the number of graph automorphisms. We then have $|\mathrm{Out}(T)| = d\epsilon g$ [Gor82, pp. 303, 304]. Thus Tables 2 and 4 enable us to find $|\mathrm{Out}(T)|$ in all cases.

We now give the proofs of Lemmas 5.5–5.7.

Proof of Lemma 5.5. Let $T = \mathrm{PSL}_2(q)$. In this case, Theorem 5 and Proposition 5.2 do not apply. Note that, for T to be simple, we require $q \geq 4$. Moreover, as $\mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5) \cong A_5$ and $\mathrm{PSL}_2(9) \cong A_6$ (see [Wil09, p. 3]), the cases $q = 4$, 5 and 9 follow from Lemma 5.3. We verify (2) for the remaining values of q.

We have

$$a(T) = \begin{cases} q+1 & \text{if } q = 2^e, \\ q & \text{if } q \text{ is odd;} \end{cases}$$

T	restrictions	d	ϵ	g
$\mathrm{PSL}_n(q)$	$n \geq 2$ $(n,q) \neq (2,2)$ $(n,q) \neq (2,3)$	$(n, q-1)$	e	1 if $n = 2$ 2 if $n > 2$
$\mathrm{PSU}_n(q)$	$n \geq 3$ $(n,q) \neq (3,2)$	$(n, q+1)$	$2e$	1
$\mathrm{PSp}_{2n}(q)$	$n \geq 2$ $(n,q) \neq (4,2)$	$(2, q-1)$	e	2 if $n = 2$ and q is even 1 otherwise
$\mathrm{P}\Omega_{2n+1}(q)$	$n \geq 3$	$(2, q-1)$	e	1
$\mathrm{P}\Omega^+_{2n}(q)$	$n \geq 4$	$(4, q^n-1)$	e	6 if $n = 4$ 2 otherwise
$\mathrm{P}\Omega^-_{2n}(q)$	$n \geq 4$	$(4, q^n+1)$	$2e$	1

TABLE 2. Automorphisms of classical simple groups of Lie type

T	$\lvert G\rvert$
$G_2(q)$ $(q \geq 3)$	$q^6(q^6-1)(q^2-1)$
$F_4(q)$	$q^{24}(q^{12}-1)(q^8-1)(q^6-1)(q^2-1)$
$E_6(q)$	$q^{36}(q^{12}-1)(q^9-1)(q^8-1)(q^6-1)(q^5-1)(q^2-1)$
${}^2E_6(q)$	$q^{36}(q^{12}-1)(q^9+1)(q^8-1)(q^6-1)(q^5+1)(q^2-1)$
${}^3D_4(q)$	$q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$
$E_7(q)$	$q^{63}(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^{10}-1)(q^8-1)(q^6-1)(q^2-1)$
$E_8(q)$	$q^{120}(q^{30}-1)(q^{24}-1)(q^{20}-1)(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^8-1)(q^2-1)$
${}^2B_2(q)$ $(q = 2^{2n+1}$ $n \geq 1)$	$q^2(q^2+1)(q-1)$
${}^2G_2(q)$ $(q = 3^{2n+1}$ $n \geq 1)$	$q^3(q^3+1)(q-1)$
${}^2F_4(q)$ $(q = 2^{2n+1}$ $n \geq 1)$	$q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$
${}^2F_4(2)'$	$q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$ with $q = 2$

TABLE 3. Exceptional simple groups of Lie type

see [Vdo99, Theorem 3.1] or the full list of subgroups of T in [Hup79, 8.27]. Also, $|\mathrm{Out}(T)| = de$ with $d = (q-1, 2)$ by Table 2 (or [Wil09, Theorem 3.2, p. 50]).

If $q = 2^e$ with $e \geq 3$, then $d = 1$, $|T| = q(q^2-1)$, $|\mathrm{Out}(T)| = e$ and $a(T) = q+1$. Thus $a(\mathrm{Aut}(T)) \leq (q+1)e$. So it suffices to show that $3^{1/3}(q+1)^2 e < q(q^2-1)$, which will follow from $3^{1/3}e < q-2$. The last inequality holds for $e = 3$ (so $q = 8$), and hence for all $e \geq 3$.

T	d	ϵ	g
$G_2(q)$	1	e	2 if $q = 3^e$ 1 otherwise
$F_4(q)$	1	e	2 if $q = 2^e$ 1 otherwise
$E_6(q)$	$(3, q-1)$	e	2
${}^2E_6(q)$	$(3, q+1)$	$2e$	1
${}^3D_4(q)$	1	$3e$	1
$E_7(q)$	$(2, q-1)$	e	1
$E_8(q)$	1	e	1
${}^2B_2(q)$	1	e	1
${}^2G_2(q)$	1	e	1
${}^2F_4(q)$	1	e	1
${}^2F_4(2)'$	2	1	1

TABLE 4. Automorphisms of exceptional simple groups of Lie type

For odd $q > 3$, we have $d = 2$, $|\mathrm{Out}(T)| = 2e$, $|T| = \frac{1}{2}q(q^2-1)$ and $a(T) = q$. It therefore suffices to show that

$$3^{1/3} \cdot 2eq^2 < \tfrac{1}{2}q(q^2-1),$$

which will follow from

$$3^{1/3} \cdot 4e < q - 1.$$

This holds for $q = p^e$ if $p \geq 7$, $e \geq 1$, if $p = 5$, $e \geq 2$ and $p = 3$, $e \geq 3$. Hence (4) holds in all cases. □

In the proofs of the remaining two lemmas, we will frequently use the fact that, for any prime power $q = p^e$, $e \geq 1$, we have $e^3 \leq \frac{1}{2}q^2$. We also note that, since $|T| = |G|/d$, the inequality (4) to be proved may be rewritten as

$$3d|\mathrm{Out}(T)|^3 < |G|. \tag{5}$$

Proof of Lemma 5.6. Let T be a classical group of Lie type which is not of the form $\mathrm{PSL}_2(q)$. We consider each family in Table 1.

For $T = \mathrm{PSL}_n(q)$ with $n \geq 3$, we have $d \leq q-1$, $g = 2$ so that

$$|\mathrm{Out}(T)| \leq 2(q-1)e.$$

Thus

$$3d|\mathrm{Out}(T)|^3 \leq 24(q-1)^4e^3 \leq 12(q-1)^4q^2.$$

If $n \geq 4$ then $|G| > q^{12}$ so $3d|\mathrm{Out}(T)|^3 < 2^4q^6 < |G|$. If $n = 3$ then $|G| > q^7(q-1)$, so that $3d|\mathrm{Out}(T)|^3 < 12q^5(q-1) < |G|$ provided that $q \geq 4$. For $n = 3$ and $q = 2$ or 3, we have $d = 1$ so that

$$3d|\mathrm{Out}(T)|^3 = 24e^3 \leq 12q^2 < q^6 < |G|.$$

Thus (5) holds for all the simple groups $\mathrm{PSL}_n(q)$.

For $T = \mathrm{PSU}_n(q)$, we have $d \leq q+1 \leq \frac{3}{2}q$ and

$$3d|\mathrm{Out}(T)|^3 \leq 3(q+1)^4(2e)^3.$$

So if $n \geq 4$ then

$$3d|\mathrm{Out}(T)|^3 \leq 3\left(\tfrac{3}{2}q\right)^4(2e)^3 < 2^6q^6 < q^{12} < |G|.$$

Now let $n = 3$ (so $q \geq 3$). Then $|G| > q^7(q-1)$, and, since $d \leq q+1 \leq \frac{4}{3}q$, we have

$$3d|\mathrm{Out}(T)|^3 \leq 3\left(\tfrac{4}{3}q\right)^4(2e)^3 < 40q^6.$$

Thus (5) holds if $q \geq 7$, since then $q(q-1) > 40$. It remains to check the cases $q = 3$, 4 and 5. We have $d = 1$ for $q = 3$, 4, and $d = 3$ for $q = 5$. Also $e = 1$ for $q = 3$, 5 and $e = 2$ for $q = 4$. Hence $|\mathrm{Out}(T)| = 2de \leq 6$ for $q \leq 5$, so that $3d|\mathrm{Out}(T)|^3 \leq 9 \cdot 6^3 < 3^7 < |G|$.

For $T = \mathrm{PSp}_{2n}(q)$ or $\mathrm{P\Omega}_{2n+1}(q)$, we have $d \leq 2$, $g \leq 2$ so

$$3d|\mathrm{Out}(T)|^3 \leq 3 \cdot 2^7e^3 \leq 3 \cdot 2^6q^2 \leq \tfrac{3}{4}q^{10} < |G|,$$

where the last inequality holds as the case $(n, q) = (2, 2)$ does not occur.

For $T = \mathrm{P\Omega}^+_{2n}(q)$ or $T = \mathrm{P\Omega}^-_{2n}(q)$, we have $d \leq 4$, and in both cases $|\mathrm{Out}(T)| = d\epsilon g \leq 24e$. Thus

$$3d|\mathrm{Out}(T)|^3 \leq 12 \cdot (24e)^3 \leq 2^{10} \cdot 3^4q^2 < 2^{17}q^2 \leq q^{19} < |G|. \qquad \square$$

Proof of Lemma 5.7. Let T be an exceptional group of Lie type. From Table 4, we have $d \leq 3$ and $|\mathrm{Out}(T)| \leq 6e$ in all cases. Thus it suffices to prove that $9(6e)^3 < |G|$. This inequality will hold if

$$4 \cdot 3^5q^2 < |G| \tag{6}$$

Now for $q \geq 2$, we have $4 \cdot 3^5 < q^{10}$, so (6) will hold if $|G| > q^{12}$. From Table 3, this covers all cases except ${}^2B_2(q)$ and ${}^2G_2$. For these two cases, we have $d = 1$ and $|\mathrm{Out}(T)| = e$, so that we only need to show $3e^3 < |G|$. But as $e^3 < q^2$ we have $3e^3 < q^3 < |G|$ in both cases. Thus the inequality (5) holds for all the exceptional groups of Lie type. $\square$

This concludes the proof of Theorem 4, and so concludes our first proof of Theorem 2.

6. Second proof of Theorem 2

In this section, we give a more direct proof of Theorem 2, using [Li03, Lemma 3.2], which in turn depends on a result of Ito [Ito55, Satz 1] on groups which are a product of two abelian subgroups. For the reader's convenience, we include proofs of both these results.

Lemma 6.1 (Ito)**.** *Let $G = AB$ be a group which is the product of two abelian subgroups A, B. Then G is metabelian.*

Proof. First note that as $G = AB$ we also have $G = BA$. (If $g^{-1} = ab$ with $a \in A$, $b \in B$ then $g = b^{-1}a^{-1}$.)

Let H be the subgroup of G generated by all commutators of the form $aba^{-1}b^{-1}$ with $a \in A$, $b \in B$. We will show that H is both normal in G and abelian. It is then immediate that G/H is also abelian, so that G is metabelian (and indeed H is the derived subgroup of G).

Given $a, \alpha \in A$ and $b, \beta \in B$, write $\alpha b\alpha^{-1} = b_1a_1$ and $\beta a\beta^{-1} = a_2b_2$, with $a_1, a_2 \in A$ and $b_1, b_2 \in B$. Then

$$\alpha(aba^{-1}b^{-1})\alpha^{-1} = ab_1a^{-1}b_1^{-1} \in H, \tag{7}$$

and

$$\beta(aba^{-1}b^{-1})\beta^{-1} = a_2ba_2^{-1}b^{-1} \in H. \tag{8}$$

Since A and B generate H, (7) and (8) show that H is normal in G.

Conjugating (7) by β and using $\beta a\beta^{-1} = a_2b_2$ to eliminate a, we obtain

$$\beta\alpha aba^{-1}b^{-1}\alpha^{-1}\beta^{-1} = a_2b_1a_2^{-1}b_1^{-1}. \tag{9}$$

Conjugating (8) by α and using $\alpha b\alpha^{-1} = b_1a_1$ to eliminate b, we obtain

$$\alpha\beta aba^{-1}b^{-1}\beta^{-1}\alpha^{-1} = a_2b_1a_2^{-1}b_1^{-1}. \tag{10}$$

It follows from (9) and (10) that $aba^{-1}b^{-1}$ and $\alpha^{-1}\beta^{-1}\alpha\beta$ commute. Since $a, \alpha \in A$ and $b, \beta \in B$ are arbitrary, this shows that H is abelian. □

Lemma 6.2 (Li)**.** *Let Y be a transitive permutation group on a set Ω and suppose that Y contains an insoluble regular normal subgroup R. Then Y contains no abelian regular subgroup.*

Proof. Let G be an abelian regular subgroup of Y, and let $W = \langle R, G\rangle$. Then $W = RG$ since R is normal in Y. Let $\omega \in \Omega$. Since R and G are regular, we have

$$W = RW_\omega = GW_\omega.$$

Using the normality of R again, we then have

$$W_\omega \cong W/R = RG/R \cong G/(R \cap G).$$

Thus W is the product of two abelian subgroups G and W_ω. Hence, by Lemma 6.1, W is metabelian, and, in particular, soluble. This is impossible since its subgroup R is insoluble. □

Proof of Theorem 2. Suppose that L/K is a finite Galois extension of fields with $\Gamma = \mathrm{Gal}(L/K)$ abelian, and that L/K admits a Hopf–Galois structure of insoluble type G. Then we have a regular embedding of Γ into $\mathrm{Hol}(G)$. Now $\mathrm{Hol}(G)$ is transitive on G and contains an insoluble regular normal subgroup, namely the group $\lambda(G)$ of left translations by G. Since the image of Γ in $\mathrm{Hol}(G)$ is an abelian regular subgroup, this contradicts Lemma 6.2. □

Remark 6.3. We now explain why we believe that our first proof of Theorem 2, despite its length and complexity, may still be of value in future work on Hopf–Galois structures. Essentially the strategy of the first proof is to break G into characteristically simple subquotients $J \cong T^m$, where T is a simple group, and where J occurs as the type of a Hopf–Galois structure on a Galois extension of fields whose group Δ is a subquotient of Γ (and hence is abelian). We then eliminate all possibilities for the simple group T except the abelian ones, so that $J = C_p^m$ for some prime p and some $m \geq 1$. If we have in mind a particular family of abelian groups Γ, we may have additional information on the groups J. For example, if Γ is cyclic, then so is Δ, and we find that a cyclic extension of degree p^m must admit a Hopf–Galois structure of elementary abelian type. By known results on Hopf–Galois structures for cyclic extensions of prime-power degree [Koh98, Byo07], this can only happen if $m = 1$ or $p^m = 4$. It follows that if a cyclic extension admits a Hopf–Galois structure of type G, then there is a chain of subgroups $1 = G_0 \subset G_1 \subset \cdots \subset G_r = G$ such that each G_j is characteristic in G and the order of each quotient G_j/G_{j-1} is either a prime or 4. This is a much stronger restriction on the structure of G than solubility alone. On the other hand, if we slightly relax the condition that Γ be abelian by considering groups with an abelian normal subgroup of index at most k (for some fixed, small k), we can again reduce to the situation where G is characteristically simple. It seems likely that arguments similar to those of §5 could then be used to eliminate all nonabelian potential composition factors of G with a few exceptions (depending on k).

7. Cases where the composition factors differ

In this section, we show that a Galois extension with group Γ may admit Hopf–Galois structures of type G, where the composition factors of the groups Γ and G differ. In particular, we shall prove Theorem 3 and Corollary 1.1. All our examples arise from the construction we shall give in Lemma 7.1.

Two subgroups H, J in a finite group G are said to be complementary if $|H|\,|J| = |G|$ and $H \cap J = \{e_G\}$. (We do not require either subgroup to be normal.) Then each element of G can be written uniquely in the form hj with $h \in H$ and $j \in J$. If G acts faithfully and transitively as permutations of some set X, and H is the stabilizer of an element of X, then a subgroup J of G is complementary to H if and only if J is regular on X. In particular, if G contains a Hall p'-subgroup H for some prime p then (taking X to be the space of left cosets of H), any Sylow p-subgroup of G is complementary to H.

Lemma 7.1. *Suppose that G contains a pair of complementary subgroups H, J. Then any Galois extension of fields with Galois group $\Gamma = H \times J$ admits a Hopf–Galois structure of type G.*

Proof. It suffices to exhibit a regular embedding $\beta : H \times J \longrightarrow \mathrm{Hol}(G)$. Using the notation of (1), we claim that such an embedding is given by the formula $\beta(h, j) = [hj^{-1}, C(j)]$ for $h \in H$, $j \in J$ where, for any $g \in G$, $C(g) \in \mathrm{Aut}(G)$ is conjugation by g, that is, $C(g)(x) = gxg^{-1}$ for $x \in G$. More concisely, $\beta(h, j)(x) = hj^{-1}(jxj^{-1}) = hxj^{-1}$ for $x \in G$.

We check that β is indeed a homomorphism. If h_1, $h_2 \in H$ and j_1, $j_2 \in J$, then, for each $x \in G$, we calculate

$$\beta(h_1, j_1)\beta(h_2, j_2)(x) = h_1(h_2 x j_2^{-1})j_1^{-1} = (h_1h_2)x(j_1j_2)^{-1} = \beta(h_1h_2, j_1j_2)(x)$$

so that $\beta(h_1, j_1)\beta(h_2, j_2) = \beta(h_1h_2, j_1j_2)$ as required. The homomorphism β is regular since each $x \in G$ can be written uniquely in the form hj^{-1} with $h \in H$ and $j \in J$. □

Remark 7.2. Lemma 7.1 is an application of the method of fixed-point free pairs of homomorphisms; see [BC12, §2] (or, in the case that $\Gamma = G$, [CCo07, §4]). For finite groups Γ, G of the same order, we say that homomorphisms

$$\beta_1, \beta_2 \colon \Gamma \longrightarrow G$$

form a fixed-point free pair if $\beta_1(\sigma) = \beta_2(\sigma)$ only for $\sigma = e_\Gamma$. We then have a regular embedding $\beta \colon \Gamma \longrightarrow \mathrm{Hol}(G)$ given by

$$\beta(\sigma) = \lambda(\beta_1(\sigma))\rho(\beta_2(\sigma)) = [\beta_1(\sigma)\beta_2(\sigma)^{-1}, C(\beta_2(\sigma))],$$

where $\lambda, \rho \colon G \longrightarrow \mathrm{Hol}(G)$ are the regular left and right embeddings, $\lambda(\sigma)(\tau) = \sigma\tau$, $\rho(\sigma)(\tau) = \tau\sigma^{-1}$ for $\tau \in G$. In the proof of Lemma 7.1, we have $\beta_1, \beta_2 \colon H \times J \longrightarrow G$ with $\beta_1(h, j) = h$ and $\beta_2(h, j) = j$.

Before proving Theorem 3, we consider the case of symmetric and alternating groups.

Example 7.3. Let $G = S_n$ for $n \geq 3$, and let $H = S_{n-1}$, the stabilizer of a point in the usual action of S_n on n points. Let J be the cyclic group generated by any n-cycle in S_n. Then J is regular on the n points, and hence is complementary to H. Thus, by Lemma 7.1, any Galois extension with group $\Gamma = S_{n-1} \times C_n$ admits a Hopf Galois structure of type S_n. If $n \geq 5$ then S_n has the simple group A_n as a composition factor, whereas Γ does not.

Example 7.4. Let $G = A_n$ with $n \geq 5$, odd, and let $H = A_{n-1}$, the stabilizer of a point. As n is odd, A_n contains an n-cycle, and again this generates a complement J to H. Thus any Galois extension with group $\Gamma = A_{n-1} \times C_n$ admits a Hopf–Galois structure of type A_n.

For even n, the case $G = A_n$ is a little more involved.

Lemma 7.5. *Let $n \geq 4$ with $n \not\equiv 2 \bmod 4$. Write $n = 2^e m$ with $m \geq 1$ odd. Then any Galois extension with group $\Gamma = A_{n-1} \times C_2^e \times C_m$ admits a Hopf–Galois structure of type A_n.*

Proof. When n is odd (so $e = 0$), the result follows from Example 7.4. So suppose $e \geq 2$. We view A_n as permuting the elements of the finite group $B = C_2^e \times C_m$ of order n. We write B additively. The group $\lambda(B)$ of left translations by elements of B is a regular subgroup of $\mathrm{Perm}(B) \cong S_n$. If $0 \neq v \in C_2^e$, then left translation by $(v, 0) \in B$ swaps the elements of B in pairs. Thus, as a product of disjoint cycles, $\lambda(v, 0)$ consists of $n/2$ transpositions. As $n/2$ is even, $\lambda(v, 0)$ is an even permutation. Similarly, $\lambda(0, 1)$ is a product of 2^e m-cycles, which is again an even permutation as m is odd. But B is generated by the elements $(v, 0)$ for $0 \neq v \in C_2^e$ and $(0, 1)$, so $\lambda(B)$ lies in A_n. Thus $J = \lambda(B)$ is a complementary subgroup to A_{n-1} in A_n, and we may again apply Lemma 7.1. □

Remark 7.6. If $n \equiv 2 \bmod 4$, then there is no complementary subgroup J to A_{n-1} in A_n. To see this, observe that J would have to be a regular subgroup, so that any element of J of order 2 would consist of $n/2$ transpositions, and therefore could not be in A_n.

We now turn to the proof of Theorem 3. We will need the following result of Guralnick [Gur83, Theorem 1], which depends on the classification of finite simple groups.

Theorem 6 (Guralnick)**.** *Let G be a finite nonabelian simple group with a subgroup H of prime-power index, $|G : H| = p^a > 1$. Then one of the following holds.*

(i) *$G = A_n$ with $n = p^a \geq 5$ and $H = A_{n-1}$.*
(ii) *$G = \mathrm{PSL}_n(q)$ and H is the stabilizer of a point or hyperplane in the action of G on the projective space $\mathbb{P}^{n-1}(\mathbb{F}_q)$; here*
$$|G : H| = (q^n - 1)/(q - 1) = p^a.$$
(iii) *$G = \mathrm{PSL}_2(11)$ and $H = A_5$.*
(iv) *G is the Matthieu group M_{23} or M_{11}, and $H = M_{22}$ or M_{10}, respectively.*
(v) *$G = \mathrm{PSU}_4(2) \cong \mathrm{PSp}_4(3)$ and H is a maximal parabolic subgroup of $\mathrm{PSU}_4(2)$ of index 27.*

Moreover, H is a Hall p'-subgroup of G except in case (i) with $n = p^a > p$ and in case (v).

Proof of Theorem 3. We consider the various cases in Theorem 6. In case (i), the result follows from Lemma 7.5. In cases (ii), (iii) and (iv), the group H is a Hall p'-subgroup. Taking J to be a Sylow p-subgroup of H, so that H, J are complementary subgroups in G, the result follows from Lemma 7.1.

It remains to consider case (v), where H is not a Hall p'-subgroup. Let $G = \mathrm{PSU}_4(2)$. As the factor d in Table 2 is $(n, q + 1) = (4, 3) = 1$ in this case, $G \cong \mathrm{SU}_4(2)$. Let $V = \mathbb{F}_4^4$, and label the standard ordered basis of row vectors as e_1, f_1, e_2, f_2. We endow V with the sesquilinear form $(\cdot, \cdot)$ where
$$(e_i, e_j) = (f_i, f_j) = 0, \qquad (e_i, f_j) = \delta_{ij}.$$

Then we may take G to be the subgroup of $\mathrm{SL}_4(4)$ which preserves this form. More concretely, G consists of the matrices M over $\mathbb{F}_4$ of determinant 1 such that $MF\overline{M} = F$, where

$$F = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

and, for any matrix M, we write $\overline{M}$ for the transpose of the matrix obtained by applying the involution $x \mapsto \overline{x} = x^2$ of $\mathbb{F}_4$ to each entry of M. Without loss of generality, we take H to the stabilizer in G of the maximal isotropic subspace $W = \mathbb{F}_4 e_1 + \mathbb{F}_4 e_2$ of V. Let X be the set of all 2-dimensional isotropic subspaces of V. Then G acts transitively on X, and a calculation confirms that indeed $|X| = 27$. Thus we need to show that there is a subgroup of G which acts regularly on X. Such a group will have order 27, whereas a Sylow 3-subgroup of G has order 81.

Let $\omega \in \mathbb{F}_4$ with $\omega^2 + \omega + 1 = 0$, and consider the matrices

$$A = \begin{pmatrix} 1 & \omega & 1 & \omega^2 \\ \omega^2 & 1 & \omega & 1 \\ 1 & \omega^2 & 1 & \omega \\ \omega^2 & \omega & \omega & \omega^2 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

One verifies by direct calculation that $A, B \in G$ and that $A^9 = B^3 = I \neq A^3$ and $BAB^{-1} = A^4$. Thus A and B generate a subgroup J of G of order 27. Moreover, the images of W under the 10 matrices A^m, $0 \leq m \leq 8$ and B are all distinct. (The image of W in each case is the $\mathbb{F}_4$-span of rows 1 and 3 of the matrix.) Since the size of the orbit of W under J must be a factor of $|J|$, it follows that J is transitive, and hence regular, on X as required. □

Proof of Corollary 1.1. (i) This follows from Theorem 3 (or Example 7.4) on taking $G = A_5$ and $H = A_4$.

(ii) Let $G = \mathrm{PSL}_3(2) \cong \mathrm{PSL}_2(7)$ of order 168. The stabilizer H of a point (or line) in the projective plane $\mathbb{P}^2(\mathbb{F}_2)$ has index 7 and order 24. By [Hup79, 8.27], we have $H \cong S_4$. The result then follows from Lemma 7.1.

(iii) Let $p = 2^e - 1$ be a Mersenne prime, and let $G = \mathrm{PSL}_2(p)$. The stabilizer H of a point in $\mathbb{P}^1(\mathbb{F}_p)$ under the action of G has index $p+1 = 2^e$ and order $\frac{1}{2}p(p-1)$. In particular, H is a Hall $2'$-subgroup of G, so a Sylow 2-subgroup J will be complementary to H. From [Hup79, 8.27], $H \cong F_{\frac{1}{2}p(p-1)}$ and $J \cong D_{2^e}$, so again Lemma 7.1 gives the required result. □

Acknowledgement. The author would like to thank Griff Elder and Henri Johnston for helpful comments on an earlier version of this paper.

References

[Byo96] 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, *ibid.* 3705. MR1405283 (97j:16051b).

[Byo97] Byott, Nigel P. Galois structure of ideals in wildly ramified abelian p-extensions of a p-adic field, and some applications. *J. Théor. Nombres Bordeaux* **9** (1997), no. 1, 201–219. MR1469668 (98h:11152), Zbl 0889.11040, doi: 10.5802/jtnb.196.

[Byo04a] Byott, Nigel P. Hopf–Galois structures on Galois field extensions of degree pq. *J. Pure Applied Algebra* **188** (2004), no. 1–3, 45–57. MR2030805 (2004j:16041), Zbl 1047.16022, doi: 10.1016/j.jpaa.2003.10.010.

[Byo04b] 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.

[Byo07] 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.

[BC12] Byott, Nigel P.; Childs, Lindsay N. Fixed-point free pairs of homomorphisms and nonabelian Hopf–Galois structures. *New York J. Math.* **18** (2012), 707–731. MR2991421, Zbl 1282.12002.

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

[CS69] Chase, Stephen U.; Sweedler, Moss E. Hopf algebras and Galois theory. Lecture Notes in Mathematics, 97. *Springer-Verlag, Berlin-New York*, 1969. ii+133 pp. MR0260724 (41 #5348), Zbl 0197.01403, doi: 10.1007/BFb0101435.

[Chi89] Childs, Lindsay N. On the Hopf Galois theory for separable field extensions. *Comm. Algebra* **17** (1989), no. 4, 809–825. MR0990979 (90g:12003), Zbl 0692.12007, doi: 10.1080/00927878908823760.

[Chi00] 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, doi: 10.1090/surv/080.

[Chi05] Childs, Lindsay N. Elementary abelian Hopf Galois structures and polynomial formal groups. *J. Algebra* **283** (2005), no. 1, 292–316. MR2102084 (2005g:16073), Zbl 1071.16031, doi: 10.1016/j.jalgebra.2004.07.009.

[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.

[CRV15] Crespo, Teresa; Rio, Anna; Vela, Montserrat. Non-isomorphic Hopf Galois structures with isomorphic underlying Hopf algebras. *J. Algebra* **422** (2015), 270–276. MR3272077, Zbl 06370252, arXiv:1406.5054, doi: 10.1016/j.jalgebra.2014.07.038.

[CRVa] Crespo, Teresa; Rio, Anna; Vela, Montserrat. The Hopf Galois property in subfield lattices. Preprint, 2013. arXiv:1309.5754.

[CRVb] Crespo, Teresa; Rio, Anna; Vela, Montserrat. From Galois to Hopf Galois: theory and practice. Preprint, 2014. arXiv:1403.6300.

[Gor82] Gorenstein, Daniel. Finite simple groups. An introduction to their classification. University Series in Mathematics. *Plenum Publishing Corp., New York*, 1982. x+333 pp. ISBN: 0-306-40779-5. MR0698782 (84j:20002), Zbl 0483.20008.

[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.

[Gur83] Guralnick, Robert M. Subgroups of prime power index in a simple group. *J. Algebra* **81** (1983), no. 2, 304–311. MR0700286 (84m:20007), Zbl 0515.20011, doi: 10.1016/0021-8693(83)90190-4.

[Hup79] Huppert, B. Endliche Gruppen. I. Die Grundlehren der Mathematischen Wissenschaften, Band 134. *Springer-Verlag, Berlin-New York*, 1967. xii+793 pp. MR0224703 (37 #302), Zbl 0412.20002, doi: 10.1007/978-3-642-64981-3.

[Ito55] Itô, Noboru. Über das Produkt von zwei abelschen Gruppen. *Math. Z.* **62** (1955), 400–401. MR0071426 (17,125b), Zbl 0064.25203, doi: 10.1007/BF01180647.

[Koh98] 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.

[Koh13] Kohl, Timothy. Regular permutation groups of order *mp* and Hopf Galois structures. *Algebra Number Theory* **7** (2013), no. 9, 2203–2240. MR3152012, Zbl 1286.12002, doi: 10.2140/ant.2013.7.2203.

[Li03] Li, Cai Heng. The finite primitive permutation groups containing an abelian regular subgroup. *Proc. London Math. Soc.* (3) **87** (2003), no. 3, 725–747. MR2005881 (2004i:20003), Zbl 1040.20001, doi: 10.1112/S0024611503014266.

[Rob96] Robinson, Derek J. S. A course in the theory of groups. Second edition. Graduate Texts in Mathematics, 80. *Springer-Verlag, New York*, 1996. xviii+499 pp. ISBN: 0-387-94461-3. MR1357169 (96f:20001), Zbl 0836.20001, doi: 10.1007/978-1-4684-0128-8.

[Ste60] Steinberg, Robert. Automorphisms of finite linear groups. *Canad. J. Math.* **12** (1960), 606–615. MR0121427 (22 #12165), Zbl 0097.01703, doi: 10.4153/CJM-1960-054-6.

[Vdo99] Vdovin, E. P. Maximal orders of abelian subgroups in finite simple groups. *Algebra Log.* **38** (1999), no. 2, 131–160, 253; translation in *Algebra and Logic* **38** (1999), no. 2, 67–83. MR1763386 (2001g:20016), Zbl 0936.20009, doi: 10.1007/BF02671721.

[Wil09] Wilson, Robert A. The finite simple groups. Graduate Texts in Mathematics, 251. *Springer-Verlag, London, Ltd., London*, 2009. xvi+298 pp. ISBN: 978-1-84800-987-5. MR2562037 (2011e:20018), Zbl 1203.20012, doi: 10.1007/978-1-84800-988-2.

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

This paper is available via http://nyjm.albany.edu/j/2015/21-40.html.