Journal of Number Theory 214 (2020) 286–311

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

Hopf-Galois structures on finite extensions with almost simple Galois group

Cindy (Sin Yi) Tsang

School of Mathematics (Zhuhai), Sun Yat-Sen University, Zhuhai, Guangdong, China

ARTICLE INFO

Article history:
Received 13 January 2020
Received in revised form 30 April 2020
Accepted 30 April 2020
Available online 19 May 2020
Communicated by A. Pal

Keywords:
Hopf-Galois structures
Holomorph
Regular subgroups
Almost simple groups

ABSTRACT

In this paper, we study the Hopf-Galois structures on a finite Galois extension whose Galois group G is an almost simple group in which the socle A has prime index p. Each Hopf-Galois structure is associated to a group N of the same order as G. We shall give necessary criteria on these N in terms of their group-theoretic properties, and determine the number of Hopf-Galois structures associated to $A \times C_p$, where C_p is the cyclic group of order p.

Contents

E-mail address: zengshy26@mail.sysu.edu.cn.
URL: http://sites.google.com/site/cindysinyitsang/.

https://doi.org/10.1016/j.jnt.2020.04.003
0022-314X/

1. Introduction

Given a group Γ, write $\mathrm{Perm}(\Gamma)$ for its symmetric group, and recall that a subgroup $\mathcal{D}$ of $\mathrm{Perm}(\Gamma)$ is said to be *regular* if the map

$$\xi_{\mathcal{D}} : \mathcal{D} \longrightarrow \Gamma; \qquad \xi_{\mathcal{D}}(\delta) = \delta(1_\Gamma)$$

is bijective. The images of the left and right regular representations

$$\begin{cases} \lambda : \Gamma \longrightarrow \mathrm{Perm}(\Gamma); & \lambda(\gamma) = (x \mapsto \gamma x) \\ \rho : \Gamma \longrightarrow \mathrm{Perm}(\Gamma); & \rho(\gamma) = (x \mapsto x\gamma^{-1}) \end{cases}$$

of Γ are examples of regular subgroups of $\mathrm{Perm}(\Gamma)$. Recall also that

$$\mathrm{Hol}(\Gamma) = \rho(\Gamma) \rtimes \mathrm{Aut}(\Gamma)$$

is the *holomorph* of Γ. Alternatively, it is easy to check that

$$\mathrm{Norm}(\lambda(\Gamma)) = \mathrm{Hol}(\Gamma) = \mathrm{Norm}(\rho(\Gamma)),$$

where $\mathrm{Norm}(-)$ denotes the normalizer in $\mathrm{Perm}(\Gamma)$.

Given a finite Galois extension L/K with Galois group G, by work of [11], we know that the number of *Hopf-Galois structures* on L/K is equal to

$$e(G) = \#\{\text{regular subgroups of } \mathrm{Perm}(G) \text{ normalized by } \lambda(G)\}.$$

In particular, for each group N having the same order as G, the number of Hopf-Galois structures on L/K of *type* N is equal to

$$e(G, N) = \# \left\{ \begin{array}{c} \text{regular subgroups of } \mathrm{Perm}(G) \text{ which are} \\ \text{isomorphic to } N \text{ and normalized by } \lambda(G) \end{array} \right\}. \tag{1.1}$$

By [3], this finer count may be calculated via the formula

$$e(G, N) = \frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(N)|} \cdot \# \left\{ \begin{array}{c} \text{regular subgroups of } \mathrm{Hol}(N) \\ \text{which are isomorphic to } G \end{array} \right\}. \tag{1.2}$$

The computation of $e(G, N)$ has been a problem of interest in the literature; see [1,4,6, 14,15,20] for some related work. We shall refer the reader to [9, Chapter 2] for a more detailed discussion on Hopf-Galois structures.

This paper is motivated by the case when G is the symmetric group S_n for $n \geq 5$. First, by [8, Theorems 5 and 9], we know that

$$e(S_n, S_n) = 2 + 2 \cdot \#\{\sigma \in A_n : \sigma \text{ has order } 2\}, \tag{1.3}$$

$$e(S_n, A_n \times C_2) = 2 \cdot \#\{\sigma \in S_n \setminus A_n : \sigma \text{ has order } 2\}, \tag{1.4}$$

where A_n is the alternating group and C_2 is the cyclic group of order 2. Also see [8, Corollaries 6 and 10], which give explicit formulae in terms of n for these two numbers. The case $n = 6$ is slightly different because S_6 is not the full automorphism group of A_6, and as noted on [8, p. 91], we have

$$e(S_6, \mathrm{PGL}_2(9)) = 0 \text{ and } e(S_6, \mathrm{M}_{10}) = 72, \tag{1.5}$$

where M_{10} is the Mathieu group of degree 10. Recently, the present author has shown in [21] that in fact

$$e(S_n, N) \neq 0 \text{ only if } N \simeq \begin{cases} S_n, A_n \times C_2 & \text{for } n \neq 6, \\ S_6, A_6 \times C_2, \mathrm{M}_{10}, \mathrm{PGL}_2(9) & \text{for } n = 6. \end{cases} \tag{1.6}$$

Hence, the number $e(S_n, N)$ is known for every group N of order $n!$.

Recall that a group Γ is said to be *almost simple* if

$$A \leq \Gamma \leq \mathrm{Aut}(A) \text{ for some non-abelian simple group } A,$$

where A is identified with its inner automorphism group $\mathrm{Inn}(A)$, and in this case A is the socle of Γ. For $n \geq 5$, the symmetric group S_n is almost simple with socle A_n of index 2. Note also that $\mathrm{PGL}_2(9)$ and M_{10} are almost simple groups with socle A_6 of index 2.

The purpose of this paper is to investigate to what extent the results (1.3), (1.4), and (1.6) for the symmetric groups may be generalized to an arbitrary finite almost simple group in which its socle has prime index.

Notation. In the rest of this paper, assume that G is a finite almost simple group with socle A such that A has prime index p in G. Note that then

$$A \text{ is the unique non-trivial proper normal subgroup of } G. \tag{1.7}$$

Also, we shall use the symbol N to denote a group of the same order as G.

For (1.3), as shown in [22, Theorem 1.3], we already know:

Theorem 1.1. *We have*

$$e(G,G) = 2 + 2 \cdot \#\{\sigma \in A : \sigma \text{ has order } p\} + 2 \cdot \frac{p-2}{p-1} \cdot \#\{\sigma \in G \setminus A : \sigma \text{ has order } p\},$$

provided that $\mathrm{Inn}(G)$ *is the only subgroup isomorphic to* G *in* $\mathrm{Aut}(G)$.

For (1.4), in Section 4, we shall prove:

Theorem 1.2. *We have*

$$e(G, A \times C_p) = 2 \cdot \frac{1}{p-1} \cdot \#\{\sigma \in G \setminus A : \sigma \text{ has order } p\},$$

where C_p *is the cyclic group of order* p.

Recall that a group Γ is *perfect* if it equals its own commutator subgroup $[\Gamma, \Gamma]$, and *quasisimple* if it is perfect and $\Gamma/Z(\Gamma)$ is simple, where $Z(\Gamma)$ is the center of Γ.

For (1.6), we shall study the cases when N is non-perfect and perfect separately. In Sections 5 and 6, respectively, we shall prove:

Theorem 1.3. *If* N *is non-perfect and* $e(G,N) \neq 0$, *then* $N \simeq A \times C_p$ *or* N *is an almost simple group with socle isomorphic to* A.

Theorem 1.4. *If* N *is perfect and* $e(G,N) \neq 0$, *then all of the conditions*

(1) N *is a quasisimple group with* $N/Z(N)$ *isomorphic to* A;
(2) A *admits an automorphism having exactly* p *fixed points;*
(3) $N/Z(N)$ *has an element* $\widetilde{\zeta}Z(N)$ *of order* p *such that*

$$\eta\widetilde{\zeta} \equiv \widetilde{\zeta}\eta \pmod{Z(N)} \text{ implies } \eta\widetilde{\zeta} = \widetilde{\zeta}\eta \text{ for all } \eta \in N;$$

hold, and in the case that $Z(N)$ *is fixed pointwise by* $\mathrm{Aut}(N)$, *the condition*

(4) A *has an element* ζ *of order* p *such that*

$$\sigma\zeta = \zeta\sigma \text{ for some } \sigma \in G \setminus A;$$

holds as well.

For $n \geq 5$, we know that $\mathrm{Inn}(S_n)$ is the only subgroup isomorphic to S_n in $\mathrm{Aut}(S_n)$. This is because $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$ for $n \neq 6$ and was proven in [16] for $n = 6$. Also,

when $N = 2A_n$ is the double cover of A_n, condition (3) in Theorem 1.4 fails by the proof of [21, Lemma 2.7]. Hence, Theorems 1.1 to 1.4 imply the case when G is S_n.

The converse of Theorem 1.3 is false by (1.5). By Theorem 1.2, we have

$$e(G, A \times C_p) \neq 0 \text{ if and only if } G \text{ splits over } A \text{ as a group extension.}$$

However, the author does not know whether there is any simple criterion on an almost simple N with socle isomorphic to A such that $e(G, N) \neq 0$. Also, she does not know whether there exist any examples of G and perfect N for which all four conditions in Theorem 1.4 are satisfied. It is possible that in fact $e(G, N) = 0$ for all perfect N, but currently we are unable to prove this, and the conditions in Theorem 1.4 might not be sufficient to rule out these N. But observe that if $e(G, N) \neq 0$ with N perfect, then p divides the order of the Schur multiplier of A by condition (1) in Theorem 1.4. Since p divides the order of the outer automorphism group of A by hypothesis, this already gives restrictions on G. We shall discuss more applications of our theorems in Section 7.

Finally, let us make one remark. The following is due to N. P. Byott.

Conjecture 1.5. *Given any finite groups Γ and Δ of the same order, if Γ is insolvable and $e(\Gamma, \Delta) \neq 0$, then Δ is also insolvable.*

It is known that Conjecture 1.5 is true when Γ is non-abelian simple [5] and when Γ is the double cover of A_n for $n \geq 5$ [19]. Recently, it was further shown in [23] that Conjecture 1.5 holds when the order of Γ and Δ is cubefree, less than 2000, or satisfy some suitable conditions. Our Theorem 1.3 implies that Conjecture 1.5 is true when Γ is almost simple in which the socle has prime index. Let us remark that in the preprint [24], the author has also extended the result of [5] to the case when Γ is quasisimple.

2. Preliminaries

In this section, let Γ be a finite group.

2.1. Regular subgroups in the holomorph

Let Δ be a finite group, not necessarily of the same order as Γ. Let us recall some known methods which may be used to study regular subgroups of $\mathrm{Hol}(\Gamma)$.

Definition 2.1. We have the following definitions.

(1) Given any $\mathfrak{f} \in \mathrm{Hom}(\Delta, \mathrm{Aut}(\Gamma))$, a map $\mathfrak{g}$ from Δ to Γ is said to be a *crossed homomorphism with respect to* $\mathfrak{f}$ if

$$\mathfrak{g}(\delta_1\delta_2) = \mathfrak{g}(\delta_1) \cdot \mathfrak{f}(\delta_1)(\mathfrak{g}(\delta_2)) \text{ for all } \delta_1, \delta_2 \in \Delta. \tag{2.1}$$

Write $Z^1_{\mathfrak{f}}(\Delta, \Gamma)$ for the set of all such crossed homomorphisms.

(2) Given any $\varphi, \psi \in \mathrm{Hom}(\Delta, \Gamma)$, a *fixed point* of (φ, ψ) is an element $\delta \in \Delta$ such that $\varphi(\delta) = \psi(\delta)$, and (φ, ψ) is said to be *fixed point free* if it has no fixed point other than 1_Δ.

Proposition 2.2. *The regular subgroups of* $\mathrm{Hol}(\Gamma)$ *isomorphic to* Δ *are precisely the subsets of the shape*

$$\mathcal{D} = \{\rho(\mathfrak{g}(\delta)) \cdot \mathfrak{f}(\delta) : \delta \in \Delta\}$$

as $\mathfrak{f}$ *ranges over* $\mathrm{Hom}(\Delta, \mathrm{Aut}(\Gamma))$ *and* $\mathfrak{g}$ *over the bijective maps in* $Z^1_{\mathfrak{f}}(\Delta, \Gamma)$.

Proof. This follows directly from the definition that $\mathrm{Hol}(\Gamma) = \rho(\Gamma) \rtimes \mathrm{Aut}(\Gamma)$; or see [19, Proposition 2.1] for a proof. □

Proposition 2.3. *Given* $\mathfrak{f} \in \mathrm{Hom}(\Delta, \mathrm{Aut}(\Gamma))$ *and* $\mathfrak{g} \in Z^1_{\mathfrak{f}}(\Delta, \Gamma)$*, define*

$$\mathfrak{h} : \Delta \longrightarrow \mathrm{Aut}(\Gamma); \qquad \mathfrak{h}(\delta) = \mathrm{conj}(\mathfrak{g}(\delta)) \cdot \mathfrak{f}(\delta), \tag{2.2}$$

where $\mathrm{conj}(-) = \lambda(-)\rho(-)$*. Then:*

(a) The map $\mathfrak{h}$ *is a homomorphism.*
(b) The fixed points of $(\mathfrak{f}, \mathfrak{h})$ *are precisely the elements of* $\mathfrak{g}^{-1}(Z(\Gamma))$.
(c) For all $\delta_1 \in \ker(\mathfrak{f})$ *and* $\delta_2 \in \Delta$*, we have* $\mathfrak{g}(\delta_1\delta_2) = \mathfrak{g}(\delta_1)\mathfrak{g}(\delta_2)$.
(d) For all $\delta_1 \in \ker(\mathfrak{h})$ *and* $\delta_2 \in \Delta$*, we have* $\mathfrak{g}(\delta_1\delta_2) = \mathfrak{g}(\delta_2)\mathfrak{g}(\delta_1)$.

Proof. See [22, Proposition 3.4] for (a) and the rest are easily verified. Let us just note that for (b), by definition $\delta \in \Delta$ is a fixed point of $(\mathfrak{f}, \mathfrak{h})$ if and only if $\mathrm{conj}(\mathfrak{g}(\delta)) = \mathrm{Id}_\Gamma$, which is equivalent to $\mathfrak{g}(\delta) \in Z(\Gamma)$. □

Recall that a subgroup Λ of Γ is *characteristic* if $\varphi(\Lambda) = \Lambda$ for all $\varphi \in \mathrm{Aut}(\Gamma)$. In this case, clearly Λ is normal in Γ, and

$$\mathrm{Aut}(\Gamma) \longrightarrow \mathrm{Aut}(\Gamma/\Lambda); \qquad \varphi \mapsto (x\Lambda \mapsto \varphi(x)\Lambda)$$

is a well-defined homomorphism.

Proposition 2.4. *Let* Λ *be a characteristic subgroup of* Γ*. Given*

$$\mathfrak{f} \in \mathrm{Hom}(\Delta, \mathrm{Aut}(\Gamma)) \text{ and } \mathfrak{g} \in Z^1_{\mathfrak{f}}(\Delta, \Gamma),$$

they induce two canonical maps

$$\overline{\mathfrak{f}}_\Lambda : \Delta \longrightarrow \mathrm{Aut}(\Gamma) \longrightarrow \mathrm{Aut}(\Gamma/\Lambda) \text{ and } \overline{\mathfrak{g}}_\Lambda : \Delta \longrightarrow \Gamma \longrightarrow \Gamma/\Lambda,$$

respectively, via compositions with the map $\mathrm{Aut}(\Gamma) \longrightarrow \mathrm{Aut}(\Gamma/\Lambda)$ *above and the natural quotient map* $\Gamma \longrightarrow \Gamma/\Lambda$. *Then:*

(a) We have $\overline{\mathfrak{f}}_\Lambda \in \mathrm{Hom}(\Delta, \mathrm{Aut}(\Gamma/\Lambda))$ *and* $\overline{\mathfrak{g}}_\Lambda \in Z^1_{\overline{\mathfrak{f}}_\Lambda}(\Delta, \Gamma/\Lambda)$.
(b) The subset $\mathfrak{g}^{-1}(\Lambda)$ *is a subgroup of* Δ.
(c) In the case that $\mathfrak{g}$ *is bijective, there is a regular subgroup of* $\mathrm{Hol}(\Lambda)$ *which is isomorphic to* $\mathfrak{g}^{-1}(\Lambda)$.

Proof. Both (a) and (b) are clear; see [19, Lemma 4.1] for a proof of (b). For part (c), see [23, Proposition 3.3]. □

Following [5] or [19, Section 4], we shall apply Proposition 2.4 to a maximal characteristic subgroup Λ of Γ. In this case, the quotient Γ/Λ is a finite non-trivial characteristically simple group, and so we know that

$$\Gamma/\Lambda \simeq T^m, \text{ where } T \text{ is a finite simple group and } m \in \mathbb{N}. \tag{2.3}$$

This shall be a crucial step in the proof of Theorems 1.3 and 1.4.

2.2. Some group-theoretic facts

We shall need the following basic properties of groups in which there is a normal copy of A of index p.

Lemma 2.5. *Assume that* Γ *has a normal subgroup* Λ *isomorphic to* A *and* $[\Gamma : \Lambda] = p$. *Then, either* $\Gamma \simeq \Lambda \times C_p$ *or* Γ *is almost simple with socle* Λ.

Proof. Since Λ is normal in Γ, we have a homomorphism

$$\Phi : \Gamma \longrightarrow \mathrm{Aut}(\Lambda); \qquad \Phi(\gamma) = (x \mapsto \gamma x \gamma^{-1}).$$

Put $C = \ker(\Phi)$, which is the centralizer of Λ in Γ, and $C \cap \Lambda = 1$ because Λ has trivial center. If $C \neq 1$, then since $[\Gamma : \Lambda] = p$, we deduce that

$$\Gamma = \Lambda C = \Lambda \times C \text{ and } C \simeq C_p.$$

If $C = 1$, then Γ embeds into $\mathrm{Aut}(\Lambda)$ via Φ, and since $\Phi(\Lambda) = \mathrm{Inn}(\Lambda)$, this implies that Γ is almost simple with socle Λ. □

Lemma 2.6. *Assume that* $\Gamma = A \times C_p$. *Then:*

(a) The non-trivial proper normal subgroups of Γ *are exactly* A *and* C_p.
(b) The subgroups A *and* C_p *of* Γ *are characteristic.*

(c) We have $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(A) \times \mathrm{Aut}(C_p)$.

Proof. Let Λ be any normal subgroup of Γ. Note that $\Lambda \cap A$ is normal in A. Since A is simple, there are only two possibilities.

- $\Lambda \cap A = A$: Then $A \subset \Lambda$, so $\Lambda = A$ or $\Lambda = \Gamma$ since A has prime index in Γ.
- $\Lambda \cap A = 1$: Then Λ has exponent dividing p. The projection of Λ onto A, which is normal in A, hence cannot be A and so must be trivial. It follows that $\Lambda \subset C_p$, so $\Lambda = 1$ or $\Lambda = C_p$.

This proves (a), which in turn implies (b) and then (c). □

Lemma 2.7. *Assume that* Γ *is almost simple with socle* A*. Then:*

(a) The center of Γ *is trivial;*
(b) The group $\mathrm{Aut}(\Gamma)$ *embeds into* $\mathrm{Aut}(A)$ *via restriction to* A*.*

Proof. This is well-known; or see [22, Lemmas 4.1 and 4.3] for a proof. □

The next lemma gives some consequences of the classification of finite simple groups which we shall need.

Lemma 2.8. *Assume that* Γ *is non-abelian simple. Then:*

(a) The outer automorphism $\mathrm{Out}(\Gamma)$ *of* Γ *is solvable.*
(b) Every $\varphi \in \mathrm{Aut}(\Gamma)$ *has a fixed point other than* 1_Γ*.*
(c) There is no subgroup isomorphic to Γ *in* $\mathrm{Aut}(\Gamma)$ *other than* $\mathrm{Inn}(\Gamma)$*.*

Proof. See [10, Theorems 1.46 and 1.48] and [22, Corollary 5.3]. □

3. The case when N has a normal copy of A

In this section, assume that N contains A as a normal subgroup. In this case we have $[N : A] = p$ because N is assumed to have the same order as G. Then, by Lemma 2.5, either $N \simeq A \times C_p$ or N is almost simple with socle A. We shall prove an alternative formula for the number $e(G, N)$ which is similar to but not quite the same as (1.2).

3.1. A key observation

Let us first prove:

Proposition 3.1. *A regular subgroup* $\mathcal{G}$ *of* $\mathrm{Hol}(N)$ *isomorphic to* G*, which is not equal to* $\lambda(N)$ *or* $\rho(N)$*, is normalized by exactly one of* $\lambda(N)$ *and* $\rho(N)$*.*

Let $\mathcal{G}$ be a regular subgroup of $\mathrm{Hol}(N)$ isomorphic to G which is not equal to $\lambda(N)$ or $\rho(N)$. By Proposition 2.2, we know that

$$\mathcal{G} = \{\rho(\mathfrak{g}(\sigma)) \cdot \mathfrak{f}(\sigma) : \sigma \in G\}, \text{ where } \begin{cases} \mathfrak{f} \in \mathrm{Hom}(G, \mathrm{Aut}(N)), \\ \mathfrak{g} \in Z^1_{\mathfrak{f}}(G, N) \text{ is bijective.} \end{cases}$$

We may also rewrite it as

$$\mathcal{G} = \{\lambda(\mathfrak{g}(\sigma))^{-1} \cdot \mathfrak{h}(\sigma) : \sigma \in G\}, \text{ where } \mathfrak{h} \in \mathrm{Hom}(G, \mathrm{Aut}(N)) \tag{3.1}$$

is defined as in (2.2). Note that both $\mathfrak{f}$ and $\mathfrak{h}$ are non-trivial because

$$\begin{cases} \mathcal{G} \subset \rho(N) & \text{if } \mathfrak{f} \text{ were trivial,} \\ \mathcal{G} \subset \lambda(N) & \text{if } \mathfrak{h} \text{ were trivial,} \end{cases}$$

in which case we would have equality by the bijectivity of $\mathfrak{g}$. From (1.7), we then deduce that $\ker(\mathfrak{f})$ and $\ker(\mathfrak{h})$ are either trivial or equal to A.

Lemma 3.2. *The following are true.*

(a) If $\mathfrak{f}$ is injective, then $\mathcal{G}$ is not normalized by $\rho(N)$.
(b) If $\mathfrak{h}$ is injective, then $\mathcal{G}$ is not normalized by $\lambda(N)$.

Proof. Suppose that $\mathfrak{f}$ is injective. For any $\sigma \in G$ and $\eta \in N$, we have

$$\rho(\eta) \cdot \rho(\mathfrak{g}(\sigma))\mathfrak{f}(\sigma) \cdot \rho(\eta)^{-1} = \rho(\eta\mathfrak{g}(\sigma)\mathfrak{f}(\sigma)(\eta)^{-1}) \cdot \mathfrak{f}(\sigma).$$

By the injectivity of $\mathfrak{f}$, the above element lies in $\mathcal{G}$ if and only if

$$\eta\mathfrak{g}(\sigma)\mathfrak{f}(\sigma)(\eta)^{-1} = \mathfrak{g}(\sigma), \text{ or equivalently } \mathfrak{h}(\sigma)(\eta) = \eta.$$

But $\mathfrak{h}$ is non-trivial and so $\mathcal{G}$ is not normalized by $\rho(G)$. This proves (a), and a similar argument using (3.1) shows (b). □

Note that A is characteristic in N. This is Lemma 2.6(b) if $N \simeq A \times C_p$ and is because A is the socle of N if N is almost simple. Hence, we have

$$\overline{\mathfrak{f}}_A, \overline{\mathfrak{h}}_A \in \mathrm{Hom}(G, \mathrm{Aut}(N/A)) \quad \text{and} \quad \overline{\mathfrak{g}}_A \in Z^1_{\overline{\mathfrak{f}}_A}(G, N/A)$$

defined as in Proposition 2.4 and (2.2). Note that

$$\mathrm{Aut}(N/A) \simeq \mathrm{Aut}(C_p) \simeq C_{p-1} \text{ (cyclic group of order } p-1).$$

This, together with (1.7), implies that $\overline{\mathfrak{f}}_A$ is trivial, and so $\overline{\mathfrak{g}}_A$ is a homomorphism by Proposition 2.3(c). But $N/A \simeq C_p$, and $\overline{\mathfrak{g}}_A$ is surjective because $\mathfrak{g}$ is bijective. Again from (1.7), we see that $\ker(\overline{\mathfrak{g}}_A) = A$, which gives $\mathfrak{g}(A) = A$. This equality shall be important in the arguments that follow. Note that $\overline{\mathfrak{h}}_A$ is trivial similarly by (1.7).

For any $\sigma \in G$ and $\eta \in N$, since $\overline{\mathfrak{f}}_A$ and $\overline{\mathfrak{h}}_A$ are trivial, we have

$$\eta \cdot \mathfrak{f}(\sigma)(\eta)^{-1} \in A \text{ and } \eta \cdot \mathfrak{h}(\sigma)(\eta)^{-1} \in A.$$

Since $\mathfrak{g}(A) = A$, there exist $\sigma_{\eta,\mathfrak{f}}, \sigma_{\eta,\mathfrak{h}} \in A$ such that

$$\mathfrak{g}(\sigma_{\eta,\mathfrak{f}}) = \eta \cdot \mathfrak{f}(\sigma)(\eta)^{-1} \text{ and } \mathfrak{g}(\sigma_{\eta,\mathfrak{h}}) = \eta \cdot \mathfrak{h}(\sigma)(\eta)^{-1}.$$

Let us rewrite the above as

$$\begin{aligned} \mathfrak{g}(\sigma_{\eta,\mathfrak{f}})\mathfrak{g}(\sigma)^{-1} &= \eta\mathfrak{g}(\sigma)^{-1}\mathfrak{h}(\sigma)(\eta)^{-1}, \\ \mathfrak{g}(\sigma_{\eta,\mathfrak{h}})\mathfrak{g}(\sigma) &= \eta\mathfrak{g}(\sigma)\mathfrak{f}(\sigma)(\eta)^{-1}. \end{aligned}$$

We may now prove the next lemmas.

Lemma 3.3. *The following are true.*

(a) If $\ker(\mathfrak{f}) = A$*, then* $\mathcal{G}$ *is normalized by* $\rho(N)$*.*
(b) If $\ker(\mathfrak{h}) = A$*, then* $\mathcal{G}$ *is normalized by* $\lambda(N)$*.*

Proof. Suppose that $\ker(\mathfrak{f}) = A$. For any $\sigma \in G$ and $\eta \in N$, we have

$$\rho(\eta) \cdot \rho(\mathfrak{g}(\sigma))\mathfrak{f}(\sigma) \cdot \rho(\eta)^{-1} = \rho(\mathfrak{g}(\sigma_{\eta,\mathfrak{h}})\mathfrak{g}(\sigma)) \cdot \mathfrak{f}(\sigma),$$

where $\sigma_{\eta,\mathfrak{h}} \in A$. Since $\ker(\mathfrak{f}) = A$, from Proposition 2.3(c), we deduce that

$$\rho(\mathfrak{g}(\sigma_{\eta,\mathfrak{h}})\mathfrak{g}(\sigma)) \cdot \mathfrak{f}(\sigma) = \rho(\mathfrak{g}(\sigma_{\eta,\mathfrak{h}}\sigma)) \cdot \mathfrak{f}(\sigma_{\eta,\mathfrak{h}}\sigma),$$

whence $\mathcal{G}$ is normalized by $\rho(N)$. This proves (a). A similar argument using (3.1) and Proposition 2.3(d) shows (b). □

Lemma 3.4. *The kernels* $\ker(\mathfrak{f})$ *and* $\ker(\mathfrak{h})$ *are not both trivial or both* A*.*

Proof. Recall from Proposition 2.3(b) that $\mathfrak{g}^{-1}(Z(N))$, which has size $|Z(N)|$ because $\mathfrak{g}$ is bijective, is precisely the set of fixed points of $(\mathfrak{f}, \mathfrak{h})$. We have

$$Z(N) = \begin{cases} C_p & \text{if } N \simeq A \times C_p, \\ 1 & \text{if } N \text{ is almost simple with socle } A, \end{cases}$$

where the latter holds by Lemma 2.7(a). Then, clearly $\ker(\mathfrak{f})$ and $\ker(\mathfrak{h})$ are not both A, because elements of $\ker(\mathfrak{f}) \cap \ker(\mathfrak{h})$ are fixed points of $(\mathfrak{f}, \mathfrak{h})$.

Suppose for contradiction that both $\mathfrak{f}$ and $\mathfrak{h}$ are injective. If $N \simeq A \times C_p$, then in the notation of Lemma 2.6(c), both $\mathfrak{f}(A), \mathfrak{h}(A) \simeq A$ project trivially onto $\mathrm{Aut}(C_p) \simeq C_{p-1}$, whence they lie in $\mathrm{Aut}(A)$. If N is almost simple with socle A, then $\mathrm{Aut}(N)$ embeds into $\mathrm{Aut}(A)$ by Lemma 2.7(b). In both cases, we deduce from Lemma 2.8(c) that $\mathfrak{f}(A) = \mathfrak{h}(A)$, which we shall denote by $\mathfrak{A}$. Then, via restriction $\mathfrak{f}$ and $\mathfrak{h}$ induce isomorphisms

$$\mathrm{res}(\mathfrak{f}), \mathrm{res}(\mathfrak{h}) : A \longrightarrow \mathfrak{A}, \text{ and } \mathrm{res}(\mathfrak{f})^{-1} \circ \mathrm{res}(\mathfrak{h}) \in \mathrm{Aut}(A).$$

The set of fixed points of $\mathrm{res}(\mathfrak{f})^{-1} \circ \mathrm{res}(\mathfrak{h})$ is equal to $\mathfrak{g}^{-1}(Z(N)) \cap A$, which is trivial because $\mathfrak{g}(A) = A$. This contradicts Lemma 2.8(b). □

Proof of Proposition 3.1. To summarize, we have shown:

- If $\ker(\mathfrak{h}) = 1$ and $\ker(\mathfrak{f}) = A$, then $\mathcal{G}$ is normalized by $\rho(N)$ but not $\lambda(N)$.
- If $\ker(\mathfrak{f}) = 1$ and $\ker(\mathfrak{h}) = A$, then $\mathcal{G}$ is normalized by $\lambda(N)$ but not $\rho(N)$.

Moreover, these are the only possibilities, and so the claim follows. □

3.2. An alternative formula

Let us now prove:

Proposition 3.5. *We have*

$$e(G, N) = 2 \cdot \# \left\{ \begin{array}{c} \textit{regular subgroups of } \mathrm{Hol}(G) \textit{ other than } \lambda(G) \\ \textit{which are isomorphic to } N \textit{ and normalized by } \lambda(G) \end{array} \right\}.$$

We shall prove this using (1.1) directly. Given a subgroup $\mathcal{N}$ of $\mathrm{Perm}(G)$, denote by $\mathcal{N}^\star$ its centralizer in $\mathrm{Perm}(G)$. In the case that $\mathcal{N}$ is regular:

- $\mathcal{N}^\star \simeq \mathcal{N}$ and $(\mathcal{N}^\star)^\star = \mathcal{N}$;
- $\mathcal{N}^\star$ is also regular;
- $\mathcal{N} = \mathcal{N}^\star$ if and only if $\mathcal{N}$ is abelian;
- $\mathcal{N}$ is normalized by $\lambda(G)$ if and only $\mathcal{N}^\star$ is normalized by $\lambda(G)$.

These facts are all easy to prove; see [18, Lemmas 2.1 and 2.3], for example. Since N is non-abelian, we see that the regular subgroups of $\mathrm{Perm}(G)$ which are isomorphic to N and normalized by $\lambda(G)$ come in pairs.

Lemma 3.6. *Let $\mathcal{N}$ be any regular subgroup of* $\mathrm{Perm}(G)$ *which is isomorphic to N and normalized by $\lambda(G)$. If $\mathcal{N}$ is not equal to $\lambda(G)$ or $\rho(G)$, then exactly one of $\mathcal{N}$ and $\mathcal{N}^\star$ lies in* $\mathrm{Hol}(G)$.

Proof. The bijection $\xi_{\mathcal{N}}$ as in the introduction induces an isomorphism

$$\Xi_{\mathcal{N}} : \mathrm{Perm}(\mathcal{N}) \longrightarrow \mathrm{Perm}(G); \qquad \Xi_{\mathcal{N}}(\pi) = \xi_{\mathcal{N}} \circ \pi \circ \xi_{\mathcal{N}}^{-1}$$

under which $\lambda(\mathcal{N})$ is sent to $\mathcal{N}$. Note that $\rho(\mathcal{N})$ is the centralizer of $\lambda(\mathcal{N})$ in $\mathrm{Perm}(\mathcal{N})$ and so is sent to $\mathcal{N}^\star$. Let $\mathcal{G}$ denote the preimage of $\lambda(G)$ under $\Xi_{\mathcal{N}}$, which is a regular subgroup of $\mathrm{Perm}(\mathcal{N})$ isomorphic to G. In summary:

$$\Xi_{\mathcal{N}} : \qquad \lambda(\mathcal{N}) \mapsto \mathcal{N}, \;\; \rho(\mathcal{N}) \mapsto \mathcal{N}^\star, \;\; \mathcal{G} \mapsto \lambda(G).$$

Recall that $\mathrm{Hol}(\mathcal{N})$ is the normalizer of $\lambda(\mathcal{N})$ in $\mathrm{Perm}(\mathcal{N})$. Since $\lambda(G)$ normalizes $\mathcal{N}$, we see that $\mathcal{G}$ lies in $\mathrm{Hol}(\mathcal{N})$. Similarly, we have

$$\begin{aligned} \mathcal{N} \text{ normalizes } \lambda(G) &\iff \lambda(\mathcal{N}) \text{ normalizes } \mathcal{G}, \\ \mathcal{N}^\star \text{ normalizes } \lambda(G) &\iff \rho(\mathcal{N}) \text{ normalizes } \mathcal{G}. \end{aligned}$$

If $\mathcal{N}$ is not equal to $\lambda(G)$ or $\rho(G)$, then $\mathcal{G}$ is not equal to $\lambda(\mathcal{N})$ or $\rho(\mathcal{N})$, and the above together with Proposition 3.1 show that exactly one of $\mathcal{N}$ and $\mathcal{N}^\star$ normalizes $\lambda(G)$. The claim now follows. □

Proof of Proposition 3.5. Define

$$\begin{aligned} \kappa(N) &= \#\left(\{\lambda(G), \rho(G)\} \cap \{\text{groups isomorphic to } N\}\right) \\ &= \begin{cases} 2 & \text{if } N \simeq G, \\ 0 & \text{if } N \not\simeq G. \end{cases} \end{aligned}$$

By Lemma 3.6, the number $e(G, N)$ in (1.1) is equal to

$$\kappa(N) + 2 \cdot \# \left\{ \begin{array}{l} \text{regular subgroups of } \mathrm{Hol}(G) \text{ other than } \lambda(G), \rho(G) \\ \text{which are isomorphic to } N \text{ and normalized by } \lambda(G) \end{array} \right\}.$$

The claim is then clear. □

4. The case when $N = A \times C_p$

In this section, assume that $N = A \times C_p$, and fix a generator ϵ of C_p. We shall apply Proposition 3.5 to prove Theorem 1.2. Let us define

$$\mathrm{InHol}(G) = \rho(G) \rtimes \mathrm{Inn}(G)$$

to be the *inner holomorph* of G, which is a subgroup of $\mathrm{Hol}(G)$.

Lemma 4.1. *A regular subgroup of* $\mathrm{Hol}(G)$ *isomorphic to* N *lies in* $\mathrm{InHol}(G)$.

Proof. Let $\mathcal{N}$ be a regular subgroup of $\mathrm{Hol}(G)$ isomorphic to N. Write

$$\mathcal{N} = \{\rho(\mathfrak{g}(\eta)) \cdot \mathfrak{f}(\eta) : \eta \in N\}, \text{ where } \begin{cases} \mathfrak{f} \in \mathrm{Hom}(N, \mathrm{Aut}(G)) \\ \mathfrak{g} \in Z^1_{\mathfrak{f}}(N, G) \text{ is bijective} \end{cases}$$

as in Proposition 2.2, and let $\mathfrak{h} \in \mathrm{Hom}(N, \mathrm{Aut}(G))$ be as in (2.2). We have

$$\mathcal{N} \subset \mathrm{InHol}(G) \iff \mathfrak{f}(N) \subset \mathrm{Inn}(G) \iff \mathfrak{h}(N) \subset \mathrm{Inn}(G).$$

Since G has trivial center by Lemma 2.7(a), the pair $(\mathfrak{f}, \mathfrak{h})$ is fixed point free by Proposition 2.3(b). It follows that A cannot lie in both $\ker(\mathfrak{f})$ and $\ker(\mathfrak{h})$, so at least one of $\mathfrak{f}$ and $\mathfrak{h}$ is injective on A.

Without loss of generality, let us assume that $\mathfrak{f}$ is injective on A. By Lemmas 2.7(b) and 2.8(c), we deduce that $\mathfrak{f}(A) \simeq A$ is the subgroup of $\mathrm{Inn}(G)$ consisting of the inner automorphisms

$$\mathrm{conj}(\sigma) \in \mathrm{Inn}(G); \qquad \mathrm{conj}(\sigma)(x) = \sigma x \sigma^{-1} \qquad \text{for } \sigma \in A.$$

Put $\theta = \mathfrak{f}(\epsilon)$, which commutes with $\mathfrak{f}(A)$. But then $\sigma^{-1}\theta(\sigma)$ lies in the center of G for all $\sigma \in A$ because for any $x \in G$, we have

$$\sigma\theta(x)\sigma^{-1} = (\mathrm{conj}(\sigma) \circ \theta)(x) = (\theta \circ \mathrm{conj}(\sigma))(x) = \theta(\sigma)\theta(x)\theta(\sigma)^{-1}.$$

Since G has trivial center, we see that $\theta|_A = \mathrm{Id}_A$, so in fact $\theta = \mathrm{Id}_G$ by Lemma 2.7(b). This proves $\mathfrak{f}(N) = \mathfrak{f}(A \times C_p) = \mathfrak{f}(A)$, whence the claim. □

Now, since G has trivial center, the regular subgroups of $\mathrm{InHol}(G)$ isomorphic to N are precisely the subgroups of the shape

$$\mathcal{N}_{(f,h)} = \{\rho(h(\eta)) \cdot \lambda(f(\eta)) : \eta \in N\}$$

as f, h range over $\mathrm{Hom}(N, G)$ with (f, h) fixed point free, by [7, Proposition 6] or [19, Subsection 2.3.1]. Moreover, each $\mathcal{N}$ correspond to exactly $|\mathrm{Aut}(N)|$ pairs of (f, h). By Proposition 3.5 and Lemma 4.1, we then see that

$$e(G, N) = 2 \cdot \frac{1}{|\mathrm{Aut}(N)|} \cdot \# \left\{ \begin{array}{c} \text{fixed point free } (f, h) \text{ for } f, h \in \mathrm{Hom}(N, G) \\ \text{such that } \mathcal{N}_{(f,h)} \text{ is normalized by } \lambda(G) \end{array} \right\}.$$

In what follows, let $f, h \in \mathrm{Hom}(N, G)$. Note that both $\ker(f)$ and $\ker(h)$ are non-trivial because N is not isomorphic to G. For the pair (f, h) to be fixed point free, the subgroups

$\ker(f)$ and $\ker(h)$ must intersect trivially, whence by Lemma 2.6(a), exactly one of them is A and the other is C_p. Also, notice that by Lemma 2.8(c), we must have $h(A) = A$ if $\ker(h) = C_p$ and similarly $f(A) = A$ if $\ker(f) = C_p$.

Lemma 4.2. *Let $\mathcal{N} = \mathcal{N}_{(f,h)}$ be as above.*

(a) If $\ker(h) = C_p$ and $\ker(f) = A$, then $\mathcal{N}$ is not normalized by $\lambda(G)$.
(b) If $\ker(f) = C_p$ and $\ker(h) = A$, then $\mathcal{N}$ is normalized by $\lambda(G)$.

Proof. For any $\eta \in N$ and $\sigma \in G$, we have

$$\lambda(\sigma) \cdot \rho(h(\eta))\lambda(f(\eta)) \cdot \lambda(\sigma)^{-1} = \rho(h(\eta)) \cdot \lambda(\sigma f(\eta)\sigma^{-1}).$$

Note that $\rho(G)$ and $\lambda(G)$ intersect trivially since G has trivial center. Thus, for $\mathcal{N}$ to be normalized by $\lambda(G)$, the subgroup $f(N)$, which is non-trivial in both parts, is normal in G and in particular contains A. This yields (a).

Now, suppose that $\ker(f) = C_p$ and $\ker(h) = A$. Write $\eta = a\epsilon^i$ for $a \in A$ and $i \in \mathbb{Z}$. Since $f(A) = A$ and A is normal in G, there exists $a_\sigma \in A$ such that $f(a_\sigma) = \sigma f(a)\sigma^{-1}$. It follows that

$$\rho(h(\eta)) \cdot \lambda(\sigma f(\eta)\sigma^{-1}) = \rho(h(\epsilon^i)) \cdot \lambda(\sigma f(a)\sigma^{-1}) = \rho(h(a_\sigma \epsilon^i)) \cdot \lambda(f(a_\sigma \epsilon^i)),$$

which lies in $\mathcal{N}$. This proves (b). □

Lemma 4.3. *Suppose that $\ker(f) = C_p$ and $\ker(h) = A$. Then (f, h) is fixed point free if and only if $h(\epsilon) \notin A$.*

Proof. Again $f(A) = A$. If $h(\epsilon) \in A$, then $f(a) = h(\epsilon)$ for some $a \in A$, and so $a\epsilon \neq 1_N$ is a fixed point of (f, h). If $h(\epsilon) \notin A$, then $f(N) \cap h(N)$ is trivial, and (f, h) is fixed point free because $\ker(f) \cap \ker(h)$ is also trivial. □

Proof of Theorem 1.2. By Lemmas 4.2 and 4.3 we have

$$e(G, N) = 2 \cdot \frac{1}{|\mathrm{Aut}(N)|} \cdot e_1(G, N) \cdot e_2(G, N),$$

where we define

$$e_1(G, N) = \#\{f \in \mathrm{Hom}(N, G) : \ker(f) = C_p\},$$
$$e_2(G, N) = \#\{h \in \mathrm{Hom}(N, G) : \ker(h) = A,\ h(\epsilon) \notin A\}.$$

We have $|\mathrm{Aut}(N)| = (p-1)|\mathrm{Aut}(A)|$ by Lemma 2.6(c). Also, it is clear that

$$e_2(G, N) = \#\{\sigma \in G \setminus A : \sigma \text{ has order } p\}, \text{ and } e_1(G, N) = |\mathrm{Aut}(A)|$$

because $f(A) = A$ whenever $\ker(f) = C_p$. The theorem now follows. □

5. The case when N is non-perfect

In this section, assume that N is non-perfect and $e(G, N)$ is non-zero. We shall prove Theorem 1.3. By (1.2) and Proposition 2.2, there exist

$$\mathfrak{f} \in \mathrm{Hom}(G, \mathrm{Aut}(N)) \text{ and a bijective } \mathfrak{g} \in Z^1_{\mathfrak{f}}(G, N).$$

Since N is non-perfect, it has a maximal characteristic subgroup M containing $[N, N]$. We shall show that $M \simeq A$.

Since M contains $[N, N]$, from (2.3), we see that

$$N/M \simeq (\mathbb{Z}/\ell\mathbb{Z})^m, \text{ where } \ell \text{ is prime and } m \in \mathbb{N}.$$

Recall that $\mathfrak{f}$ and $\mathfrak{g}$, respectively, induce

$$\overline{\mathfrak{f}}_M \in \mathrm{Hom}(G, \mathrm{Aut}(N/M)) \text{ and a surjective } \overline{\mathfrak{g}}_M \in Z^1_{\overline{\mathfrak{f}}_M}(G, N/M)$$

as in Proposition 2.4. Put $H = \mathfrak{g}^{-1}(M)$, which is a subgroup of G by Proposition 2.4(b), and has order $|M|$ because $\mathfrak{g}$ is bijective. Note that

$$[A : H \cap A] = [AH : H] = \ell^m/[G : AH], \text{ and } [G : AH] = 1 \text{ or } p. \tag{5.1}$$

In the case $[G : AH] = 1$, we shall use the next lemma.

Lemma 5.1. *If A has a subgroup of index ℓ^m, then $A \simeq \mathrm{PSL}_2(7)$, or A does not embed into $\mathrm{GL}_m(\ell)$.*

Proof. See [5, Lemmas 4.2 and 4.4]. □

In the case $[G : AH] = p$, note that $\ell = p$ necessarily, and we shall use the next two lemmas. Their proofs are refinements of [5, Section 4]. A key fact is [12, Theorem 1], which gives the subgroups of prime power index in A, and its proof uses the classification of finite simple groups. We shall also use the hypothesis that A has index p in G, which means that p divides the order of the outer automorphism group $\mathrm{Out}(A)$ of A.

Lemma 5.2. *If A has a subgroup of index p^{m-1} with $m \geq 2$, then*

$$A \simeq \mathrm{PSL}_n(q) \text{ with } p^{m-1} = \frac{q^n - 1}{q - 1}, \tag{5.2}$$

or G does not embed into $\mathrm{GL}_m(p)$.

Proof. Suppose that A has a subgroup of index p^{m-1} with $m \geq 2$. Then, by [12, Theorem 1], one of the following holds.

(a) $A \simeq A_{p^{m-1}}$ with $p^{m-1} \geq 5$;
(b) $A \simeq \mathrm{PSL}_n(q)$ with $p^{m-1} = (q^n - 1)/(q - 1)$;
(c) $A \simeq \mathrm{PSL}_2(11)$ with $p^{m-1} = 11$;
(d) $A \simeq M_{11}$ with $p^{m-1} = 11$, or $A \simeq M_{23}$ with $p^{m-1} = 23$;
(e) $A \simeq \mathrm{PSU}_4(2)$ with $p^{m-1} = 27$.

Recall that p divides the order of $\mathrm{Out}(A)$. Since

$$|\mathrm{Out}(\mathrm{PSL}_2(11))| = 2 = |\mathrm{Out}(\mathrm{PSU}_4(2))|, \ \ |\mathrm{Out}(M_{11})| = 1 = |\mathrm{Out}(M_{23})|,$$

cases (c), (d), (e) do not occur. Since $|\mathrm{Out}(A_n)| = 2$ for all $n \geq 5$ with $n \neq 6$, we must have $p = 2$ with $m \geq 4$ and $G \simeq S_{2^{m-1}}$ in case (a). Notice that $S_{2^{m-1}}$ does not embed into $\mathrm{GL}_m(2)$ for $m \geq 4$ because

$$|\mathrm{GL}_m(2)| = 2^{m(m-1)/2} \cdot s \text{ with } s \in \mathbb{N} \text{ odd},$$
$$|S_{2^{m-1}}| = 2 \cdot 2^2 \cdots 2^{m-1} \cdot 6 \cdot t = 2^{m(m-1)/2+1} \cdot 3t \text{ with } t \in \mathbb{N}.$$

We are left with case (b) and the claim now follows. □

To deal with the remaining case in (5.2), we shall follow [5, Section 4] and use [13, 17], which give lower bounds for the degrees of projective irreducible representations of projective special linear groups in cross characteristics. In particular, we shall use the version stated in [5, Theorem 4.3].

Lemma 5.3. *If $A \simeq \mathrm{PSL}_n(q)$ is as in (5.2) with $m \geq 2$, then $A \simeq \mathrm{PSL}_2(7)$, or A does not embed into $\mathrm{GL}_m(p)$.*

Proof. Suppose that $A \simeq \mathrm{PSL}_n(q)$ is as in (5.2) with $m \geq 2$, and in particular

$$p^{m-1} = \frac{q^n - 1}{q - 1}. \tag{5.3}$$

We already know by [23, Lemma 4.1(a)] that A does not embed into $\mathrm{GL}_2(p)$. Hence, we may assume $m \geq 3$, and together with (5.3), we deduce that

$$(n, q) \neq (3, 2), (2, 4), (3, 4), (4, 2), (4, 3), (2, 9).$$

Suppose now that A embeds into $\mathrm{GL}_m(p)$. By [5, Theorem 4.3], we have:

- If $n \geq 3$, then $m \geq (q^n - q)/(q - 1) - 1$;

- If $n = 2$, then $m \geq (q-1)/\gcd(q-1, 2)$.

In the first case, we have

$$m \geq \frac{q^n - q}{q-1} - 1 = \frac{q^n - 1}{q-1} - 2 = p^{m-1} - 2.$$

Since $m \geq 3$, this yields $(m, p) = (3, 2)$, which cannot satisfy (5.3) for $n \geq 3$. In the second case, we have

$$m \geq \frac{q-1}{\gcd(q-1, 2)} = \frac{p^{m-1} - 2}{\gcd(p^{m-1} - 2, 2)} \geq \frac{p^{m-1} - 2}{2}.$$

Since $m \geq 3$, this yields $(m, p) = (3, 2), (4, 2)$, which corresponds to $q = 3, 7$, respectively, for $n = 2$. But $\mathrm{PSL}_2(3)$ is non-simple, so we are left with the case $A \simeq \mathrm{PSL}_2(7)$, whence the claim. □

Lemma 5.4. *If $A \not\simeq \mathrm{PSL}_2(7)$, then $\mathfrak{g}^{-1}(M) = A$ and $[N : M] = p$.*

Proof. We have $H = \mathfrak{g}^{-1}(M)$ by definition and recall the equalities in (5.1). There are three cases, and recall that $\ell = p$ necessarily when $[G : AH] = p$.

(1) $[G : AH] = 1$;
(2) $[G : AH] = p$ and $m = 1$;
(3) $[G : AH] = p$ and $m \geq 2$.

Let us first prove that $A \subset H$. In case (2), we have $[A : H \cap A] = 1$, so clearly $A \subset H$. In cases (1) and (3), suppose that $A \not\simeq \mathrm{PSL}_2(7)$. Then, since the range of $\overline{\mathfrak{f}}_M$ is equal to

$$\mathrm{Aut}(N/M) \simeq \mathrm{Aut}((\mathbb{Z}/\ell\mathbb{Z})^m) \simeq \mathrm{GL}_m(\ell),$$

we deduce from Lemma 5.1, 5.2, and 5.3 that $\overline{\mathfrak{f}}_M$ is not injective. From (1.7), it follows that $\ker(\overline{\mathfrak{f}}_M)$ has to contain A, whence $(\overline{\mathfrak{g}}_M)|_A$ is a homomorphism by Proposition 2.3(c). Since the range of $\overline{\mathfrak{g}}_M$ is equal to

$$N/M \simeq (\mathbb{Z}/\ell\mathbb{Z})^m,$$

necessarily $(\overline{\mathfrak{g}}_M)|_A$ is trivial, which means that $\mathfrak{g}(A) \subset M$, namely $A \subset H$. In all three cases, we have $A \subset H$. Since A has index p in G and $H \subsetneq G$, we must have $H = A$. This in turn implies $[N : M] = [G : A] = p$, as claimed. □

Proof of Theorem 1.3. Suppose first that $A \simeq \mathrm{PSL}_2(7)$. Then $G \simeq \mathrm{PGL}_2(7)$, and by [23, Theorem 1.10], we know that

$$e(\mathrm{PGL}_2(7), N) = 0 \text{ for all solvable } N.$$

Since $\mathrm{PGL}_2(7)$ and $\mathrm{PSL}_2(7) \times C_2$ are the only non-perfect insolvable groups of order 336, we see that Theorem 1.3 holds in this case.

Suppose now that $A \not\simeq \mathrm{PSL}_2(7)$. Then $\mathfrak{g}^{-1}(M) = A$ by Lemma 5.4, so $e(A, M) \neq 0$ by Proposition 2.4(c). Since A is non-abelian simple, by [5], this implies $M \simeq A$. Since $[N : M] = p$, the theorem follows from Lemma 2.5. □

6. The case when N is perfect

In this section, assume that N is perfect and $e(G, N)$ is non-zero. We shall prove Theorem 1.4. As in Section 5, by (1.2) and Proposition 2.2, there exist

$$\mathfrak{f} \in \mathrm{Hom}(G, \mathrm{Aut}(N)) \text{ and a bijective } \mathfrak{g} \in Z^1_{\mathfrak{f}}(G, N).$$

Also, let $\mathfrak{h} \in \mathrm{Hom}(G, \mathrm{Aut}(N))$ be defined as in (2.2). Let M be any maximal characteristic subgroup of N. We shall show that $M = Z(N)$ and $N/M \simeq A$.

Since N is perfect, from (2.3), we see that

$$N/M \simeq T^m, \text{ where } T \text{ is non-abelian simple and } m \in \mathbb{N}.$$

Recall that $\mathfrak{f}$ and $\mathfrak{g}$, respectively, induce

$$\overline{\mathfrak{f}}_M \in \mathrm{Hom}(G, \mathrm{Aut}(N/M)) \text{ and a surjective } \overline{\mathfrak{g}}_M \in Z^1_{\overline{\mathfrak{f}}_M}(G, N/M)$$

as in Proposition 2.4.

Lemma 6.1. *The group A embeds into T.*

Proof. It is known, by [5, Lemma 3.2] for example, that

$$\mathrm{Aut}(N/M) \simeq \mathrm{Aut}(T^m) \simeq \mathrm{Aut}(T)^m \rtimes S_m.$$

There exists a prime $r \neq p$ which divides $|T|$ because groups of prime power order are nilpotent. Then, since

$$p|A| = |G| = |N| = |M||T|^m, \text{ we have } r^m \text{ divides } |A|.$$

But r^m does not divide $m!$ as in the proof of [5, Lemma 3.3]. It follows that A cannot embed into S_m and so the homomorphism

$$A \xrightarrow{\overline{\mathfrak{f}}_M} \mathrm{Aut}(N/M) \xrightarrow{\text{identification}} \mathrm{Aut}(T)^m \rtimes S_m \xrightarrow{\text{projection}} S_m$$

is trivial. Since $\mathrm{Out}(T)$ is solvable by Lemma 2.8(a), the homomorphism

$$A \xrightarrow{\overline{\mathfrak{f}}_M} \mathrm{Aut}(T)^m \xrightarrow{\text{quotient}} \mathrm{Out}(T)^m$$

is also trivial. We then see that $\overline{\mathfrak{f}}_M(A)$ lies in $\mathrm{Inn}(T)^m$. Since A is simple, the homomorphism $(\overline{\mathfrak{f}}_M)|_A$ is either injective or trivial.

- If $(\overline{\mathfrak{f}}_M)|_A$ is injective, then clearly A embeds into $\mathrm{Inn}(T)^m \simeq T^m$.
- If $(\overline{\mathfrak{f}}_M)|_A$ is trivial, then $(\overline{\mathfrak{g}}_M)|_A$ is a homomorphism by Proposition 2.3(c). Note that $(\overline{\mathfrak{g}}_M)|_A$ cannot be trivial, for otherwise $A \subset \mathfrak{g}^{-1}(M)$, and

$$p = |G|/|A| \geq |G|/|\mathfrak{g}^{-1}(M)| = |N|/|M| = |T|^m,$$

  which is impossible. It follows that $(\overline{\mathfrak{g}}_M)|_A$ is injective, so A embeds into $N/M \simeq T^m$.

In both cases A embeds into T^m. But the projection of A onto the m components of T^m cannot be all trivial, so in fact A embeds into T. □

As in Section 5, we shall use [12, Theorem 1] as well as the hypothesis that A has index p in G. The former lists the subgroups of prime power index in a finite non-abelian simple group while the latter implies that p divides the order of the outer automorphism group $\mathrm{Out}(A)$ of A.

Lemma 6.2. *We have $m = 1$ and $|M| = p$.*

Proof. By Lemma 6.1, we know that A embeds into T, and write $|T| = d|A|$ for $d \in \mathbb{N}$. Then, we have

$$p|A| = |G| = |N| = |M||T|^m = d^m|A|^m|M|, \text{ and so } p = d^m|A|^{m-1}|M|.$$

This gives $m = 1$, and $|M| = 1$ or p. Suppose for contradiction that $|M| = 1$, in which case $N \simeq T$ and A embeds into T as a subgroup of index p. Since T is non-abelian simple, one of the following holds by [12, Theorem 1].

(a) $T \simeq A_p$ and $A \simeq A_{p-1}$ with $p \geq 5$;
(b) $T \simeq \mathrm{PSL}_n(q)$ with $p = (q^n - 1)/(q - 1)$;
(c) $T \simeq \mathrm{PSL}_2(11)$ and $A \simeq A_5$ with $p = 11$;
(d) $T \simeq M_{11}$ and $A \simeq M_{10}$ with $p = 11$, or $T \simeq M_{23}$ and $A \simeq \mathrm{M}_{22}$ with $p = 23$.

Note that M_{10} is non-simple. Since p divides $|\mathrm{Out}(A)|$ while

$$|\mathrm{Out}(A_n)| = 2 \text{ or } 4 \text{ for } n \geq 5 \text{ and } |\mathrm{Out}(M_{22})| = 2,$$

cases (a), (c), and (d) do not occur. To deal with case (b), observe that $N \simeq T$ has trivial center, so $(\mathfrak{f}, \mathfrak{h})$ is fixed point free by Proposition 2.3(b). Thus, the intersection

$\ker(\mathfrak{f}) \cap \ker(\mathfrak{h})$ is trivial, and by (1.7), at least one of $\mathfrak{f}$ and $\mathfrak{h}$ has to be injective. Since $\mathrm{Inn}(N) \simeq N$ has the same order but is not isomorphic to G, and by definition

$$\mathfrak{f}(G) \subset \mathrm{Inn}(N) \iff \mathfrak{h}(G) \subset \mathrm{Inn}(N),$$

the image $\mathfrak{f}(G)$ cannot lie in $\mathrm{Inn}(N) \simeq N$. It follows the homomorphism

$$G \xrightarrow{\ \mathfrak{f}\ } \mathrm{Aut}(N) \xrightarrow{\ \text{quotient}\ } \mathrm{Out}(N) \xrightarrow{\ \simeq\ } \mathrm{Out}(T)$$

is non-trivial. From (1.7), we then deduce that p has to divide $|\mathrm{Out}(T)|$. But for $n \geq 2$, by [25, Theorem 3.2] for example, we know that

$$|\mathrm{Out}(\mathrm{PSL}_n(q))| = 2\gcd(n, q-1)f \text{ or } \gcd(n, q-1)f,$$

where $q = r^f$ with r a prime. In case (b), note that

$$p = (q^n - 1)/(q-1) = q^{n-1} + \cdots + q + 1 \geq q + 1 > \max\{2, q-1, f\},$$

and we see that p cannot divide $|\mathrm{Out}(\mathrm{PSL}_n(q))|$. Hence, all four cases (a) to (d) are impossible, so necessarily $|M| = p$, as desired. □

Proof of Theorem 1.4 Condition (1). So far, we have shown that

$$A \text{ embeds into } T,\ N/M \simeq T, \text{ and } |M| = p.$$

By comparing orders, in fact $T \simeq A$. We have a homomorphism

$$N \longrightarrow \mathrm{Aut}(M); \qquad \eta \mapsto (x \mapsto \eta x \eta^{-1})$$

because M is normal. But it must be trivial since N is perfect while $\mathrm{Aut}(M)$ is cyclic. This means that $M \subset Z(N)$, and so $M = Z(N)$ by the maximality of M. Condition (1) then follows. □

Now, we know that N is quasisimple, with $N/Z(N) \simeq A$ and $|Z(N)| = p$. Using this, we may prove the next two lemmas.

Lemma 6.3. *There is no subgroup isomorphic to A in N.*

Proof. Suppose for contradiction that B is such a subgroup. Then, we have

$$|BZ(N)| = |B||Z(N)|/|B \cap Z(N)| = p|A| = |G| = |N|,$$

where $B \cap Z(N)$ is trivial because B has trivial center. But this implies that

$$N = BZ(N) \text{ and in particular } [N, N] = [B, B].$$

This is impossible because $B \subsetneq N$ and N is perfect. □

Lemma 6.4. *Both* $\mathfrak{f}$ *and* $\mathfrak{h}$ *embed* A *into* $\mathrm{Inn}(N)$.

Proof. Notice that $\mathrm{Out}(N)$ is solvable by Lemma 2.8(a); see the proof of [19, Lemma 3.6]. Since A is perfect, the homomorphisms

$$A \xrightarrow{\mathfrak{f},\mathfrak{h}} \mathrm{Aut}(N) \xrightarrow{\text{quotient}} \mathrm{Out}(N)$$

are trivial, whence $\mathfrak{f}(A)$ and $\mathfrak{h}(A)$ lie in $\mathrm{Inn}(N)$. Observe that the map

$$A \longrightarrow N; \qquad \begin{cases} x \mapsto \mathfrak{g}(x) & \text{if } \mathfrak{f}|_A \text{ were trivial} \\ x \mapsto \mathfrak{g}(x)^{-1} & \text{if } \mathfrak{h}|_A \text{ were trivial} \end{cases}$$

would be a homomorphism by Propositions 2.3(c), (d), and so A would embed into N because $\mathfrak{g}$ is bijective. But this is impossible by Lemma 6.3, so both $\mathfrak{f}$ and $\mathfrak{h}$ are injective on A, as desired. □

Lemma 6.4 tells us that $\mathfrak{f}$ and $\mathfrak{h}$, respectively, induce isomorphisms

$$f, h : A \longrightarrow N/Z(N); \qquad \begin{cases} f(\sigma) = \widetilde{f}(\sigma)Z(N), \\ h(\sigma) = \widetilde{h}(\sigma)Z(N), \end{cases}$$

where $\widetilde{f}(\sigma), \widetilde{h}(\sigma) \in N$ are such that for all $x \in N$, we have

$$\mathfrak{f}(\sigma)(x) = \widetilde{f}(\sigma)x\widetilde{f}(\sigma)^{-1} \text{ and } \mathfrak{h}(\sigma)(x) = \widetilde{h}(\sigma)x\widetilde{h}(\sigma)^{-1}.$$

Since $\mathfrak{g}$ is bijective, by Proposition 2.4(b) we know that $\mathfrak{g}^{-1}(Z(N)) = \langle\zeta\rangle$ for some $\zeta \in G$ of order p. Note also that $Z(N) = \langle\mathfrak{g}(\zeta)\rangle$.

Proof of Theorem 1.4 Condition (2). Consider $\varphi = f^{-1} \circ h$, which is an automorphism on A. For any $\sigma \in A$, we have

$$\varphi(\sigma) = \sigma \iff f(\sigma) = h(\sigma) \iff \mathfrak{f}(\sigma) = \mathfrak{h}(\sigma) \iff \sigma \in \langle\zeta\rangle \cap A$$

by Proposition 2.3(b). Since φ has a non-trivial fixed point by Lemma 2.8(b), we deduce that $\zeta \in A$, and φ has exactly p fixed points, namely the elements of $\langle\zeta\rangle$. This proves condition (2). □

Now, we also know that $\zeta \in A$, so the element $\widetilde{f}(\zeta) \in N$ is defined.

Proof of Theorem 1.4 Condition (3). Take $\widetilde{\zeta} = \widetilde{f}(\zeta)$, and $\widetilde{\zeta}Z(N) = f(\zeta)$ has order p because f is an isomorphism. Suppose for contradiction that there exists $\eta \in N$ with

$$\eta\widetilde{f}(\zeta) \equiv \widetilde{f}(\zeta)\eta \pmod{Z(N)} \text{ but } \eta\widetilde{f}(\zeta) \neq \widetilde{f}(\zeta)\eta.$$

Since $Z(N) = \langle \mathfrak{g}(\zeta) \rangle$, there exists $i \in \mathbb{Z}$ with $i \not\equiv 0 \pmod{p}$ such that

$$\widetilde{f}(\zeta)\eta\widetilde{f}(\zeta)^{-1}\eta^{-1} = \mathfrak{g}(\zeta)^i, \text{ or equivalently } \widetilde{f}(\zeta)\eta\widetilde{f}(\zeta)^{-1} = \mathfrak{g}(\zeta)^i\eta.$$

Let $j \in \mathbb{Z}$ be such that $ij \equiv -1 \pmod{p}$, and write $\eta^j = \mathfrak{g}(\sigma)$, where $\sigma \in G$. Then, since $\mathfrak{g}(\zeta) \in Z(N)$, raising the above equation to the jth power yields

$$\widetilde{f}(\zeta)\mathfrak{g}(\sigma)\widetilde{f}(\zeta)^{-1} = \mathfrak{g}(\zeta)^{-1}\mathfrak{g}(\sigma).$$

But this implies that

$$\mathfrak{g}(\zeta\sigma) = \mathfrak{g}(\zeta) \cdot \mathfrak{f}(\zeta)(\mathfrak{g}(\sigma)) = \mathfrak{g}(\zeta)\widetilde{f}(\zeta)\mathfrak{g}(\sigma)\widetilde{f}(\zeta)^{-1} = \mathfrak{g}(\sigma),$$

which contradicts that $\mathfrak{g}$ is bijective. This completes the proof of condition (3). □

Lemma 6.5. *For any $\sigma \in G$ such that $\mathfrak{f}(\sigma)$ fixes $Z(N)$ pointwise, we have*

$$\sigma\zeta = \zeta\sigma \text{ if and only if } \mathfrak{g}(\sigma)\widetilde{f}(\zeta) = \widetilde{f}(\zeta)\mathfrak{g}(\sigma).$$

Proof. In the case that $\mathfrak{f}(\sigma)$ fixes $Z(N)$ pointwise, we have

$$\begin{aligned}\mathfrak{g}(\sigma\zeta) &= \mathfrak{g}(\sigma) \cdot \mathfrak{f}(\sigma)(\mathfrak{g}(\zeta)) = \mathfrak{g}(\sigma)\mathfrak{g}(\zeta),\\ \mathfrak{g}(\zeta\sigma) &= \mathfrak{g}(\zeta) \cdot \mathfrak{f}(\zeta)(\mathfrak{g}(\sigma)) = \mathfrak{g}(\zeta)\widetilde{f}(\zeta)\mathfrak{g}(\sigma)\widetilde{f}(\zeta)^{-1}.\end{aligned}$$

Since $\mathfrak{g}$ is bijective and $\mathfrak{g}(\zeta) \in Z(N)$, we see that the claim holds. □

Let us use $\mathrm{Cent}_*(-)$ to denote the centralizer in a given group $*$.

Proof of Theorem 1.4 Condition (4). By the proof of condition (3), the map

$$\mathrm{Cent}_N(\widetilde{f}(\zeta)) \longrightarrow \mathrm{Cent}_{N/Z(N)}(f(\zeta)); \qquad \eta \mapsto \eta Z(N)$$

is surjective. Its kernel is clearly $Z(N)$, and this implies that

$$|\mathrm{Cent}_N(\widetilde{f}(\zeta))| = p \cdot |\mathrm{Cent}_{N/Z(N)}(f(\zeta))| = p \cdot |\mathrm{Cent}_A(\zeta)|,$$

where the second equality holds because f is an isomorphism. Suppose now that $Z(N)$ is fixed pointwise by $\mathrm{Aut}(N)$. Then, from Lemma 6.5, we see that

$$|\mathrm{Cent}_G(\zeta)| = |\mathrm{Cent}_N(\widetilde{f}(\zeta))|$$

since $\mathfrak{g}$ is bijective. Putting the equalities together, we obtain

$$|\mathrm{Cent}_G(\zeta)| = p \cdot |\mathrm{Cent}_A(\zeta)|,$$

from which condition (4) follows. □

7. Almost simple groups of alternating or sporadic type

In this section, let Γ be a finite almost simple group, which is non-simple, and whose socle is an alternating group or a sporadic simple group. We shall apply our theorems to determine the numbers $e(\Gamma, \Delta)$ for all groups Δ of order $|\Gamma|$, except when $\Gamma \simeq \mathrm{Aut}(A_6)$.

First, suppose that the socle of Γ is an alternating group. It is known that

$$\mathrm{Out}(A_n) \simeq C_2 \text{ for } n \geq 5 \text{ with } n \neq 6, \text{ and } \mathrm{Out}(A_6) = C_2 \times C_2.$$

Since we assumed that Γ is non-simple, either

$$\Gamma \simeq S_n \text{ with } n \geq 5, \text{ or } \Gamma \simeq \mathrm{PGL}_2(9), \mathrm{M}_{10}, \mathrm{Aut}(A_6).$$

For $\Gamma \simeq S_n$ with $n \geq 5$, the numbers $e(S_n, \Delta)$ are already known by [8] and [21]. For both $\Gamma \simeq \mathrm{PGL}_2(9), \mathrm{M}_{10}$, by Theorems 1.3 and 1.4(a), we know that

$$e(\Gamma, \Delta) \neq 0 \text{ only if } \Delta \simeq A_6 \times C_2, S_6, \mathrm{PGL}_2(9), \mathrm{M}_{10}, 2A_6,$$

where $2A_6$ is the double cover of A_6. By applying Theorems 1.1 and 1.2, we computed in Magma [2] that

$$\begin{cases} e(\mathrm{PGL}_2(9), \mathrm{PGL}_2(9)) = 92 \text{ and } e(\mathrm{PGL}_2(9), A_6 \times C_2) = 72, \\ e(\mathrm{M}_{10}, \mathrm{M}_{10}) = 92 \text{ and } e(\mathrm{M}_{10}, A_6 \times C_2) = 0. \end{cases}$$

Since $2A_6$ does not satisfy Condition (3) in Theorem 1.4, as shown in [21, Lemma 2.7] for example, we also have

$$e(\mathrm{PGL}_2(9), 2A_6) = 0 = e(\mathrm{M}_{10}, 2A_6).$$

Using (1.2) and a similar code as in the appendix of [21], we found that

$$\begin{cases} e(\mathrm{PGL}_2(9), S_6) = 0 \text{ and } e(\mathrm{PGL}_2(9), \mathrm{M}_{10}) = 60, \\ e(\mathrm{M}_{10}, S_6) = 72 \text{ and } e(\mathrm{M}_{10}, \mathrm{PGL}_2(9)) = 60. \end{cases}$$

We have thus determined $e(\Gamma, \Delta)$ completely except when $\Gamma \simeq \mathrm{Aut}(A_6)$.

Remark 7.1. Observe that

$$e(\Gamma_1, \Gamma_2) = e(\Gamma_2, \Gamma_1) \text{ for all } \Gamma_1, \Gamma_2 \in \{S_6, \mathrm{PGL}_2(9), \mathrm{M}_{10}\}$$

by the above and (1.5). These symmetries could possibly be a special case of a more general phenomenon, and perhaps come from the fact that

$$\mathrm{Aut}(A_6) \simeq \mathrm{Aut}(S_6) \simeq \mathrm{Aut}(\mathrm{PGL}_2(9)) \simeq \mathrm{Aut}(\mathrm{M}_{10}),$$

together with the formulae in (1.2) and Proposition 3.5.

Next, suppose that the socle of Γ is one of the 26 sporadic simple groups. The outer automorphism group of a sporadic simple group A has order dividing two, and is non-trivial precisely when

$$A \simeq \mathrm{M}_{12}, \mathrm{M}_{22}, \mathrm{HS}, \mathrm{J}_2, \mathrm{McL}, \mathrm{Suz}, \mathrm{He}, \mathrm{HN}, \mathrm{Fi}_{22}, \mathrm{Fi'}_{24}, \mathrm{O'N}, \mathrm{J}_3,$$

where the notation is standard. Since we assumed that Γ is non-simple, we see that $\Gamma \simeq \mathrm{Aut}(A)$ for one of the sporadic simple groups A listed above. By Theorems 1.3 and 1.4(a), we know that

$$e(\Gamma, \Delta) \neq 0 \text{ only if } \Delta \simeq A \times C_2, \mathrm{Aut}(A), \text{ or } \Delta \text{ is a double cover of } A.$$

The element structures of A as well as its covers and $\mathrm{Aut}(A)$ are available in the Atlas [26]. Using [26] and Theorem 1.1, the number $e(\Gamma, \Gamma)$ has already been computed in [22, p. 953]. Similarly, we found that

A	$e(\Gamma, A \times C_2)$ for $\Gamma \simeq \mathrm{Aut}(A)$
M_{12}	$1,584$
M_{22}	$3,432$
HS	$48,400$
J_2	$3,600$
McL	$226,800$
Suz	$5,458,752$
He	$533,120$
HN	$150,480,000$
Fi_{22}	$83,521,152$
$\mathrm{Fi'}_{24}$	$11,373,535,579,392$
O'N	$5,249,664$
J_3	$41,040$

by applying Theorem 1.2. A double cover of A exists if and only if the Schur multiplier $\mathrm{Schur}(A)$ of A has order divisible by two. Among the 12 sporadic simple groups A above, it is known that

$$\mathrm{Schur}(A) \text{ has even order } \iff A \simeq \mathrm{M}_{12}, \mathrm{M}_{22}, \mathrm{HS}, \mathrm{J}_2, \mathrm{Suz}, \mathrm{Fi}_{22}.$$

For these six sporadic simple groups A, based on [26], there is no element in $\mathrm{Aut}(A)$ whose centralizer has order 2 or 4. This implies that condition (2) in Theorem 1.4 is not satisfied, so $e(\Gamma, \Delta) = 0$ if Δ is a double cover of A. We have thus determined $e(\Gamma, \Delta)$ completely.

Acknowledgments

Research supported by the Young Scientists Fund of the National Natural Science Foundation of China (Award No.: 11901587).

The author thanks the referee for helpful comments.

References

[1] A.A. Alabdali, N.P. Byott, Counting Hopf-Galois structures on cyclic field extensions of squarefree degree, J. Algebra 493 (2018) 1–19.
[2] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, J. Symb. Comput. 24 (1997) 23–265.
[3] N.P. Byott, Uniqueness of Hopf-Galois structure of separable field extensions, Commun. Algebra 24 (10) (1996) 3217–3228, Corrigendum, Commun. Algebra 24 (11) (1996) 3705.
[4] N.P. Byott, Hopf-Galois structures on Galois field extensions of degree pq, J. Pure Appl. Algebra 188 (1–3) (2004) 45–57.
[5] N.P. Byott, Hopf-Galois structures on field extensions with simple Galois groups, Bull. Lond. Math. Soc. 36 (1) (2004) 23–29.
[6] N.P. Byott, Hopf-Galois structures on almost cyclic field extensions of 2-power degree, J. Algebra 318 (1) (2007) 351–371.
[7] N.P. Byott, L.N. Childs, Fixed-point free pairs of homomorphisms and nonabelian Hopf-Galois structures, N.Y. J. Math. 18 (2012) 707–731.
[8] S. Carnahan, L.N. Childs, Counting Hopf-Galois structures on non-Abelian Galois field extensions, J. Algebra 218 (1) (1999) 81–92.
[9] L.N. Childs, Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory, Mathematical Surveys and Monographs, vol. 80, American Mathematical Society, Providence, RI, 2000.
[10] D. Gorenstein, Finite Simple Groups: An Introduction to Their Classification, University Series in Mathematics, Plenum Publishing Corp., New York, 1982.
[11] C. Greither, B. Pareigis, Hopf-Galois theory for separable field extensions, J. Algebra 106 (1) (1987) 261–290.
[12] R.M. Guralnick, Subgroups of prime power index in a simple group, J. Algebra 81 (2) (1983) 304–311.
[13] R.M. Guralnick, P.H. Tiep, Low-dimensional representations of special linear groups in cross characteristics, Proc. Lond. Math. Soc. (3) 78 (1999) 116–138.
[14] T. Kohl, Classification of the Hopf-Galois structures on prime power radical extensions, J. Algebra 207 (2) (1998) 525–546.
[15] T. Kohl, Hopf-Galois structures arising from groups with unique subgroup of order p, Algebra Number Theory 10 (1) (2016) 37–59.
[16] T.Y. Lam, D.B. Leep, Combinatorial structure on the automorphism group of S_6, Expo. Math. 11 (4) (1993) 289–308.

[17] V. Landazuri, G.M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, J. Algebra 32 (1974) 418–443.
[18] P.J. Truman, Commuting Hopf-Galois structures on a separable extension, Commun. Algebra 46 (4) (2018) 1420–1427.
[19] C. Tsang, Non-existence of Hopf-Galois structures and bijecitive crossed homomorphisms, J. Pure Appl. Algebra 223 (7) (2019) 2804–2821.
[20] C. Tsang, Hopf-Galois structures of isomorphic type on a non-Abelian characteristically simple extension, Proc. Am. Math. Soc. 147 (12) (2019) 5093–5103.
[21] C. Tsang, Hopf-Galois structures on a Galois S_n-extension, J. Algebra 531 (1) (2019) 349–361.
[22] C. Tsang, On the multiple holomorph of a finite almost simple group, N.Y. J. Math. 25 (2019) 949–963.
[23] C. Tsang, C. Qin, On the solvability of regular subgroups in the holomorph of a finite solvable group, Int. J. Algebra Comput. 30 (2) (2020) 253–265.
[24] C. Tsang, Hopf-Galois structures on finite extensions with quasisimple Galois group, preprint, arXiv: 2001.05718.
[25] R.A. Wilson, The Finite Simple Groups, Graduate Texts in Mathematics, vol. 251, Springer-Verlag London, Ltd., London, 2009.
[26] R. Wilson, P. Walsh, J. Tripp, I. Suleiman, R. Parker, S. Norton, S. Nickerson, S. Linton, J. Bray, R. Abbott, A world-wide-web Atlas of group representations - Version 3, http://brauer.maths.qmul.ac.ul/Atlas/vs/.