Insoluble Subgroups of the Holomorph of a Finite Soluble Group

Nigel Byott

University of Exeter

Omaha, 2 June 2022

Outline

§1: The Question

Question: Can the holomorph of a finite soluble group N contain an insoluble regular subgroup?

§1: The Question

Question: Can the holomorph of a finite soluble group N contain an insoluble regular subgroup?

equivalently:

Can a finite Galois extension with insoluble Galois group G admit a Hopf-Galois structure of soluble type?

§1: The Question

Question: Can the holomorph of a finite soluble group N contain an insoluble regular subgroup?

equivalently:

Can a finite Galois extension with insoluble Galois group G admit a Hopf-Galois structure of soluble type?

or: Can a finite skew brace with soluble additive group have an insoluble multiplicative (circle) group?

§2: Some things we know:

(i) (Swapping the groups) we can have the soluble group N occurring as a regular subgroup of $\mathrm{Hol}(G)$,
e.g. $N = A_4 \times C_5$ and $G = A_5$.

§2: Some things we know:

(i) (Swapping the groups) we can have the soluble group N occurring as a regular subgroup of $\mathrm{Hol}(G)$,
e.g. $N = A_4 \times C_5$ and $G = A_5$.

(ii) We cannot have G regular in $\mathrm{Hol}(N)$ (with G insoluble, N insoluble) if $|G| = |N| < 2000$ (Tsang & Qin, 2020) or if G is a simple group (B 2004; Gorshkov & Nasybullov, 2021).

§2: Some things we know:

(i) (Swapping the groups) we can have the soluble group N occurring as a regular subgroup of $\mathrm{Hol}(G)$,
e.g. $N = A_4 \times C_5$ and $G = A_5$.

(ii) We cannot have G regular in $\mathrm{Hol}(N)$ (with G insoluble, N insoluble) if $|G| = |N| < 2000$ (Tsang & Qin, 2020) or if G is a simple group (B 2004; Gorshkov & Nasybullov, 2021).

(iii) There are no counterexamples giving bi-skew braces (Stefanello & Trappeniers, 2022).

§2: Some things we know:

(i) (Swapping the groups) we can have the soluble group N occurring as a regular subgroup of $\mathrm{Hol}(G)$,
e.g. $N = A_4 \times C_5$ and $G = A_5$.

(ii) We cannot have G regular in $\mathrm{Hol}(N)$ (with G insoluble, N insoluble) if $|G| = |N| < 2000$ (Tsang & Qin, 2020) or if G is a simple group (B 2004; Gorshkov & Nasybullov, 2021).

(iii) There are no counterexamples giving bi-skew braces (Stefanello & Trappeniers, 2022).

(iv) We can have an insoluble G as a *transitive* subgroup of $\mathrm{Hol}(N)$.
i.e. we can have a Hopf-Galois structure of soluble type on a non-normal field extension L/K whose Galois closure E has $\mathrm{Gal}(E/K) = G$.

§2: Some things we know:

(i) (Swapping the groups) we can have the soluble group N occurring as a regular subgroup of $\mathrm{Hol}(G)$,
e.g. $N = A_4 \times C_5$ and $G = A_5$.

(ii) We cannot have G regular in $\mathrm{Hol}(N)$ (with G insoluble, N insoluble) if $|G| = |N| < 2000$ (Tsang & Qin, 2020) or if G is a simple group (B 2004; Gorshkov & Nasybullov, 2021).

(iii) There are no counterexamples giving bi-skew braces (Stefanello & Trappeniers, 2022).

(iv) We can have an insoluble G as a *transitive* subgroup of $\mathrm{Hol}(N)$.
i.e. we can have a Hopf-Galois structure of soluble type on a non-normal field extension L/K whose Galois closure E has $\mathrm{Gal}(E/K) = G$.

This is easy: take $N = C_p \times C_p = \mathbb{F}_p^2$ and
$G = \mathrm{Hol}(N) = \mathbb{F}_p^2 \rtimes \mathrm{GL}_2(p)$. Then G is insoluble if $p \geq 5$.

§2: Some things we know:

(i) (Swapping the groups) we can have the soluble group N occurring as a regular subgroup of $\mathrm{Hol}(G)$,
e.g. $N = A_4 \times C_5$ and $G = A_5$.

(ii) We cannot have G regular in $\mathrm{Hol}(N)$ (with G insoluble, N insoluble) if $|G| = |N| < 2000$ (Tsang & Qin, 2020) or if G is a simple group (B 2004; Gorshkov & Nasybullov, 2021).

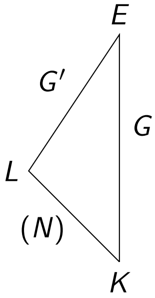
(iii) There are no counterexamples giving bi-skew braces (Stefanello & Trappeniers, 2022).

(iv) We can have an insoluble G as a *transitive* subgroup of $\mathrm{Hol}(N)$.
i.e. we can have a Hopf-Galois structure of soluble type on a non-normal field extension L/K whose Galois closure E has $\mathrm{Gal}(E/K) = G$.

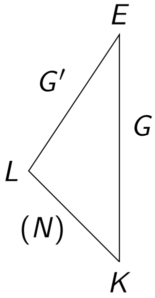
This is easy: take $N = C_p \times C_p = \mathbb{F}_p^2$ and
$G = \mathrm{Hol}(N) = \mathbb{F}_p^2 \rtimes \mathrm{GL}_2(p)$. Then G is insoluble if $p \geq 5$.

However this is uninteresting since we have just forced
$G' = \mathrm{Gal}(E/L) = \mathrm{Stab}_G(e_N)$ to be insoluble.

(v) We can have an insoluble transitive subgroup $G \leq \mathrm{Hol}(N)$ where N and G' are both soluble.



(v) We can have an insoluble transitive subgroup $G \leq \mathrm{Hol}(N)$ where N and G' are both soluble.



Example: (Crespo & Salguero, 2020)
$N = \mathbb{F}_2^3$, $G \cong \mathrm{Aut}(N) \cong \mathrm{GL}_3(2) \cong \mathrm{PSL}_2(7)$, the simple group of order 168.
In MAGMA notation $G = 8T37$.

Concretely, write

$$\mathrm{Hol}(N) = \left(\begin{array}{ccc|c} & & & * \\ & \mathrm{GL}_3(2) & & * \\ & & & * \\ \hline 0 & 0 & 0 & 1 \end{array}\right).$$

Concretely, write

$$\mathrm{Hol}(N) = \left(\begin{array}{ccc|c} & \mathrm{GL}_3(2) & & * \\ & & & * \\ & & & * \\ \hline 0 & 0 & 0 & 1 \end{array}\right).$$

Then G is generated by a subgroup G' of order 21, say

$$\left(\begin{array}{ccc|c} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), \qquad \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right)$$

Concretely, write

$$\mathrm{Hol}(N) = \left(\begin{array}{ccc|c} & \mathrm{GL}_3(2) & & \begin{matrix} * \\ * \\ * \end{matrix} \\ \hline 0 & 0 & 0 & 1 \end{array}\right).$$

Then G is generated by a subgroup G' of order 21, say

$$\left(\begin{array}{ccc|c} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), \qquad \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right)$$

and a Sylow 2-subgroup (dihedral of order 8), say

$$\left(\begin{array}{ccc|c} 1 & 1 & 0 & \\ 0 & 1 & 1 & \\ 0 & 0 & 1 & \\ \hline 0 & 0 & 0 & 1 \end{array}\right), \qquad \left(\begin{array}{ccc|c} 1 & 0 & 0 & \\ 0 & 1 & 1 & \\ 0 & 0 & 1 & \\ \hline 0 & 0 & 0 & 1 \end{array}\right).$$

Concretely, write

$$\mathrm{Hol}(N) = \left(\begin{array}{ccc|c} & \mathrm{GL}_3(2) & & \begin{matrix} * \\ * \\ * \end{matrix} \\ \hline 0 & 0 & 0 & 1 \end{array}\right).$$

Then G is generated by a subgroup G' of order 21, say

$$\left(\begin{array}{ccc|c} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), \qquad \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right)$$

and a Sylow 2-subgroup (dihedral of order 8), say

$$\left(\begin{array}{ccc|c} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), \qquad \left(\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right).$$

Up to conjugacy, this is the unique example with $G = \mathrm{GL}_3(2)$.

We can build bigger examples from this one:

$$N = \underbrace{\mathbb{F}_2^3 \times \cdots \times \mathbb{F}_2^3}_{r} = \mathbb{F}_2^{3r},$$

$$G = \underbrace{\mathrm{GL}_3(2) \times \cdots \times \mathrm{GL}_3(2)}_{r}$$

We can build bigger examples from this one:

$$N = \underbrace{\mathbb{F}_2^3 \times \cdots \times \mathbb{F}_2^3}_{r} = \mathbb{F}_2^{3r},$$

$$G = \underbrace{\mathrm{GL}_3(2) \times \cdots \times \mathrm{GL}_3(2)}_{r} \rtimes H = \mathrm{GL}_3(2) \wr H$$

where H is a transitive soluble subgroup of S_r.

§3: The main result and some reductions

Theorem:

Let (G, N) be a pair of finite groups with N soluble, G a transitive insoluble subgroup of $\mathrm{Hol}(N)$ and $G' = \mathrm{Stab}_G(1_N)$ soluble. Then

(i) if the pair (G, N) is *minimal* then there are normal subgroups $M \lhd N$ and $K \lhd G$ with K soluble such that $N/M \cong \mathbb{F}_2^3$ and $G/K = \mathrm{GL}_3(2)$;

§3: The main result and some reductions

Theorem:

Let (G, N) be a pair of finite groups with N soluble, G a transitive insoluble subgroup of $\mathrm{Hol}(N)$ and $G' = \mathrm{Stab}_G(1_N)$ soluble. Then

(i) if the pair (G, N) is *minimal* then there are normal subgroups $M \lhd N$ and $K \lhd G$ with K soluble such that $N/M \cong \mathbb{F}_2^3$ and $G/K = \mathrm{GL}_3(2)$;

(ii) if the pair (G, N) is *weakly minimal* then there are normal subgroups $M \lhd N$ and $K \lhd G$ with K soluble such that $N/M \cong \mathbb{F}_2^{3r}$ and $G/K \cong \mathrm{GL}_3(2) \wr H$ for H a transitive soluble subgroup of S_r.

§3: The main result and some reductions

Theorem:

Let (G, N) be a pair of finite groups with N soluble, G a transitive insoluble subgroup of $\mathrm{Hol}(N)$ and $G' = \mathrm{Stab}_G(1_N)$ soluble. Then

(i) if the pair (G, N) is *minimal* then there are normal subgroups $M \lhd N$ and $K \lhd G$ with K soluble such that $N/M \cong \mathbb{F}_2^3$ and $G/K = \mathrm{GL}_3(2)$;

(ii) if the pair (G, N) is *weakly minimal* then there are normal subgroups $M \lhd N$ and $K \lhd G$ with K soluble such that $N/M \cong \mathbb{F}_2^{3r}$ and $G/K \cong \mathrm{GL}_3(2) \wr H$ for H a transitive soluble subgroup of S_r.

Corollary:

For (G, N) as in the Theorem (e.g. if G is a *regular* insoluble subgroup of $\mathrm{Hol}(N)$) then the simple group $\mathrm{GL}_3(2)$ of order 168 occurs as a subquotient of G.

If (G, N) is minimal, then $\mathrm{GL}_3(2)$ occurs as a composition factor of G. It is the only non-abelian composition factor of G and it occurs with multiplicity 1.

§3: The main result and some reductions

Theorem:

Let (G, N) be a pair of finite groups with N soluble, G a transitive insoluble subgroup of $\mathrm{Hol}(N)$ and $G' = \mathrm{Stab}_G(1_N)$ soluble. Then

(i) if the pair (G, N) is *minimal* then there are normal subgroups $M \lhd N$ and $K \lhd G$ with K soluble such that $N/M \cong \mathbb{F}_2^3$ and $G/K = \mathrm{GL}_3(2)$;

(ii) if the pair (G, N) is *weakly minimal* then there are normal subgroups $M \lhd N$ and $K \lhd G$ with K soluble such that $N/M \cong \mathbb{F}_2^{3r}$ and $G/K \cong \mathrm{GL}_3(2) \wr H$ for H a transitive soluble subgroup of S_r.

Corollary:

For (G, N) as in the Theorem (e.g. if G is a *regular* insoluble subgroup of $\mathrm{Hol}(N)$) then the simple group $\mathrm{GL}_3(2)$ of order 168 occurs as a subquotient of G.

If (G, N) is minimal, then $\mathrm{GL}_3(2)$ occurs as a composition factor of G. It is the only non-abelian composition factor of G and it occurs with multiplicity 1.

The next task is to define *(weakly) minimal*.

Running hypothesis: G is a transitive insoluble subgroup of $\mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N)$ with G', N soluble.

For $g \in \mathrm{Hol}(N)$, write $g = (\alpha_g, \theta_g)$ with $\alpha_g \in N$ and $\theta_g \in \mathrm{Aut}(N)$.

Let $M \leq N$.

Definition: Let $M_* = \{g \in G : g \cdot 1_N \in M\} = \{g \in G : \alpha_g \in M\}$.
If M_* is a *subgroup* of G, we say M is an *admissible subgroup* of N.
This is equivalent to: $\theta_g(m) \in M$ for all $g \in M_*$ and all $m \in M$.
Then M_* acts transitively on M (with soluble kernel).

We call the pair (G, N) *minimal* if M_* is soluble for every admissible $M \lneq N$.

Running hypothesis: G is a transitive insoluble subgroup of $\mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N)$ with G', N soluble.

For $g \in \mathrm{Hol}(N)$, write $g = (\alpha_g, \theta_g)$ with $\alpha_g \in N$ and $\theta_g \in \mathrm{Aut}(N)$.

Let $M \leq N$.

Definition: Let $M_* = \{g \in G : g \cdot 1_N \in M\} = \{g \in G : \alpha_g \in M\}$.
If M_* is a *subgroup* of G, we say M is an *admissible subgroup* of N.
This is equivalent to: $\theta_g(m) \in M$ for all $g \in M_*$ and all $m \in M$.
Then M_* acts transitively on M (with soluble kernel).

We call the pair (G, N) *minimal* if M_* is soluble for every admissible $M \lneq N$.

Definition: If $\theta_g(m) \in M$ for all $g \in G$ and all $m \in M$, we say M is a *G-invariant subgroup* of N.
If also $M \lhd N$, then G acts on N/M and G/K is a transitive subgroup of $\mathrm{Hol}(N/M)$ for some $K \lhd G$.

We call the pair (G, N) *weakly minimal* if M_* is soluble for every G-invariant normal subgroup $M \lneq N$, and *irreducible* if there is no non-trivial G-invariant normal subgroup $M \lneq N$.

Given a pair (G, N) satisfying our hypothesis, we get a minimal pair (H, M) by passing to a suitable subgroup $M \leq N$.

Given a pair (G, N) satisfying our hypothesis, we get a minimal pair (H, M) by passing to a suitable subgroup $M \leq N$.

Given a (weakly) minimal pair (G, N), we can pass to an irreducible pair $(G/K, N/M)$ by quotienting out a maximal G-invariant normal subgroup $M \lhd N$. The stabiliser of $1_{N/M}$ is still soluble and, by (weak) minimality, K is soluble.

Given a pair (G, N) satisfying our hypothesis, we get a minimal pair (H, M) by passing to a suitable subgroup $M \leq N$.

Given a (weakly) minimal pair (G, N), we can pass to an irreducible pair $(G/K, N/M)$ by quotienting out a maximal G-invariant normal subgroup $M \lhd N$. The stabiliser of $1_{N/M}$ is still soluble and, by (weak) minimality, K is soluble.

Then $(G/K, N/M)$ is still (weakly) minimal. In particular, N/M has no proper non-trivial characteristic subgroups, so it is elementary abelian.

Given a pair (G, N) satisfying our hypothesis, we get a minimal pair (H, M) by passing to a suitable subgroup $M \leq N$.

Given a (weakly) minimal pair (G, N), we can pass to an irreducible pair $(G/K, N/M)$ by quotienting out a maximal G-invariant normal subgroup $M \lhd N$. The stabiliser of $1_{N/M}$ is still soluble and, by (weak) minimality, K is soluble.

Then $(G/K, N/M)$ is still (weakly) minimal. In particular, N/M has no proper non-trivial characteristic subgroups, so it is elementary abelian.

So we can reduce to the situation:

$$V = N = \mathbb{F}_p^d \text{ for some prime } p \text{ and some } d \geq 1,$$

$$G \leq \mathrm{Hol}(V) = \mathrm{Aff}(V) = V \rtimes \mathrm{GL}_r(p) \text{ is transitive and insoluble,}$$

$$G' = \mathrm{Stab}_G(0_V) \text{ is a soluble subgroup of index } p^d \text{ in } G.$$

Moreover, V is an irreducible $\mathbb{F}_p[G]$-module.

Given a pair (G, N) satisfying our hypothesis, we get a minimal pair (H, M) by passing to a suitable subgroup $M \leq N$.

Given a (weakly) minimal pair (G, N), we can pass to an irreducible pair $(G/K, N/M)$ by quotienting out a maximal G-invariant normal subgroup $M \lhd N$. The stabiliser of $1_{N/M}$ is still soluble and, by (weak) minimality, K is soluble.

Then $(G/K, N/M)$ is still (weakly) minimal. In particular, N/M has no proper non-trivial characteristic subgroups, so it is elementary abelian.

So we can reduce to the situation:

$$V = N = \mathbb{F}_p^d \text{ for some prime } p \text{ and some } d \geq 1,$$

$$G \leq \mathrm{Hol}(V) = \mathrm{Aff}(V) = V \rtimes \mathrm{GL}_r(p) \text{ is transitive and insoluble,}$$

$$G' = \mathrm{Stab}_G(0_V) \text{ is a soluble subgroup of index } p^d \text{ in } G.$$

Moreover, V is an irreducible $\mathbb{F}_p[G]$-module.

Our goal for the rest of the talk is to show that for any such pair (G, V),

$$p = 2, \qquad V = \mathbb{F}_2^{3r}, \qquad G = GL_3(2) \wr H \text{ with } H \leq S_r.$$

§4 Sketch of proof (1): Combinatorics of group actions

If $1 \neq J \lhd G$ then the orbits of J on V are all of the same size, and G/J transitively permutes these orbits. So J acts transitively on a set of size p^t where $1 \leq t \leq d$ and H/J acts transitively on a set of size p^s where $0 \leq s < d$. Both actions have soluble point stabilisers.

§4 Sketch of proof (1): Combinatorics of group actions

If $1 \neq J \lhd G$ then the orbits of J on V are all of the same size, and G/J transitively permutes these orbits. So J acts transitively on a set of size p^t where $1 \leq t \leq d$ and H/J acts transitively on a set of size p^s where $0 \leq s < d$. Both actions have soluble point stabilisers.

Applying this inductively to a composition series

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_m = G$$

of G, we find

(i) each composition factor G_i/G_{i-1} has soluble subgroup of index p^s for some $s \geq 0$;

(ii) for $i = 1$, we have $s \geq 1$, so $G_1 = C_p$ or a non-abelian simple group.

Step 2: (Representation theory $+$) Group theory

As V is irreducible, it follows from modular representation theory that G has no non-trivial normal p-subgroup.

Step 2: (Representation theory +) Group theory

As V is irreducible, it follows from modular representation theory that G has no non-trivial normal p-subgroup.

Hence G has no non-trivial *subnormal* p-subgroup. Combining with Step 1, this means that G has no non-trivial *subnormal soluble* subgroup.

Step 2: (Representation theory +) Group theory

As V is irreducible, it follows from modular representation theory that G has no non-trivial normal p-subgroup.

Hence G has no non-trivial *subnormal* p-subgroup. Combining with Step 1, this means that G has no non-trivial *subnormal soluble* subgroup.

In particular, every minimal normal subgroup of G has trivial centre, and is the direct product of isomorphic non-abelian simple groups.

Step 2: (Representation theory +) Group theory

As V is irreducible, it follows from modular representation theory that G has no non-trivial normal p-subgroup.

Hence G has no non-trivial *subnormal* p-subgroup. Combining with Step 1, this means that G has no non-trivial *subnormal soluble* subgroup.

In particular, every minimal normal subgroup of G has trivial centre, and is the direct product of isomorphic non-abelian simple groups.

Recall that the socle $\mathrm{soc}(G)$ of G is the subgroup generated by all minimal normal subgroups. Since for our G, the minimal subgroups have trivial centre, $\mathrm{soc}(G)$ is the direct product of *all* the minimal normal subgroups.

Hence

$$\mathrm{soc}(G) = T_1 \times \cdots \times T_r$$

where the T_k are non-abelian simple groups. (We don't yet know that they are all isomorphic.) Conjugation by G permutes the T_k, and the orbits give the minimal normal subgroups.

Step 2: (Representation theory +) Group theory

As V is irreducible, it follows from modular representation theory that G has no non-trivial normal p-subgroup.

Hence G has no non-trivial *subnormal* p-subgroup. Combining with Step 1, this means that G has no non-trivial *subnormal soluble* subgroup.

In particular, every minimal normal subgroup of G has trivial centre, and is the direct product of isomorphic non-abelian simple groups.

Recall that the socle $\mathrm{soc}(G)$ of G is the subgroup generated by all minimal normal subgroups. Since for our G, the minimal subgroups have trivial centre, $\mathrm{soc}(G)$ is the direct product of *all* the minimal normal subgroups.

Hence

$$\mathrm{soc}(G) = T_1 \times \cdots \times T_r$$

where the T_k are non-abelian simple groups. (We don't yet know that they are all isomorphic.) Conjugation by G permutes the T_k, and the orbits give the minimal normal subgroups.

Moreover the centraliser of $\mathrm{soc}(G)$ in G is trivial.

Step 3: Clifford theory

Let $S = \mathrm{soc}(G) \lhd G$. We study the irreducible $\mathbb{F}_p[G]$-module V as an $\mathbb{F}_p[S]$-module.

Step 3: Clifford theory

Let $S = \mathrm{soc}(G) \lhd G$. We study the irreducible $\mathbb{F}_p[G]$-module V as an $\mathbb{F}_p[S]$-module.

Simplifying assumption: $\mathbb{F}_p$ splits G, i.e. every irreducible $\mathbb{F}_p[G]$-module is irreducible over $\overline{\mathbb{F}}_p[G]$. (Then same holds for subgroups of G.)

Step 3: Clifford theory

Let $S = \mathrm{soc}(G) \lhd G$. We study the irreducible $\mathbb{F}_p[G]$-module V as an $\mathbb{F}_p[S]$-module.

Simplifying assumption: $\mathbb{F}_p$ splits G, i.e. every irreducible $\mathbb{F}_p[G]$-module is irreducible over $\overline{\mathbb{F}}_p[G]$. (Then same holds for subgroups of G.)

Let U be an irreducible $\mathbb{F}_p[S]$-submodule of V. Then gU is an irreducble $\mathbb{F}_p[S]$-module for each $g \in G$, and

$$V = \bigoplus_{i=1}^{m} g_i U$$

for some $g_1 = 1, g_2, \ldots, g_m \in G$.

Step 3: Clifford theory

Let $S = \mathrm{soc}(G) \lhd G$. We study the irreducible $\mathbb{F}_p[G]$-module V as an $\mathbb{F}_p[S]$-module.

Simplifying assumption: $\mathbb{F}_p$ splits G, i.e. every irreducible $\mathbb{F}_p[G]$-module is irreducible over $\overline{\mathbb{F}}_p[G]$. (Then same holds for subgroups of G.)

Let U be an irreducible $\mathbb{F}_p[S]$-submodule of V. Then gU is an irreducble $\mathbb{F}_p[S]$-module for each $g \in G$, and

$$V = \bigoplus_{i=1}^{m} g_i U$$

for some $g_1 = 1, g_2, \ldots, g_m \in G$.

Let J be a minimal normal subgroup of G. Then, for some $r(J) \geq 1$ and some non-abelian simple group T_J we have

$$J = T_1 \times \cdots \times T_{r(J)} \text{ with all } T_k \cong T_J.$$

Each T_k acts on each $g_i U$ (and this action might or might not be trivial).

Let $y(J)$ be the number of simple factors T_k acting non-trivially on $U = g_1 U$.

Let $z(J)$ be the number of summands $g_i U$ on which T_1 acts non-trivially.

Then $my(J) = r(J)z(J)$.

Let $y(J)$ be the number of simple factors T_k acting non-trivially on $U = g_1 U$.

Let $z(J)$ be the number of summands $g_i U$ on which T_1 acts non-trivially.

Then $my(J) = r(J)z(J)$.

Because $\mathbb{F}_p$ splits G, the irreducible $\mathbb{F}_p[S]$-module U can be written

$$U = \bigotimes_J U_J$$

where U_J is an irreducible $\mathbb{F}_p[J]$-module.

Let $y(J)$ be the number of simple factors T_k acting non-trivially on $U = g_1 U$.

Let $z(J)$ be the number of summands $g_i U$ on which T_1 acts non-trivially.

Then $my(J) = r(J)z(J)$.

Because $\mathbb{F}_p$ splits G, the irreducible $\mathbb{F}_p[S]$-module U can be written

$$U = \bigotimes_J U_J$$

where U_J is an irreducible $\mathbb{F}_p[J]$-module.

For a particular $J = T_1 \times \cdots \times T_{r(J)}$, we have

$$U_J = U_{J,1} \otimes \cdots \otimes U_{J,r(J)}$$

with $U_{J,k}$ an irreducible $\mathbb{F}_p[T_k]$-module.

Let $y(J)$ be the number of simple factors T_k acting non-trivially on $U = g_1 U$.

Let $z(J)$ be the number of summands $g_i U$ on which T_1 acts non-trivially.

Then $my(J) = r(J)z(J)$.

Because $\mathbb{F}_p$ splits G, the irreducible $\mathbb{F}_p[S]$-module U can be written

$$U = \bigotimes_J U_J$$

where U_J is an irreducible $\mathbb{F}_p[J]$-module.

For a particular $J = T_1 \times \cdots \times T_{r(J)}$, we have

$$U_J = U_{J,1} \otimes \cdots \otimes U_{J,r(J)}$$

with $U_{J,k}$ an irreducible $\mathbb{F}_p[T_k]$-module.

Let $d(T_J) \geq 2$ be minimal dimension of a non-trivial irreducible $\mathbb{F}_p[T_J]$-module. Then $y(J)$ of the $U_{J,j}$ are non-trivial and have dimension $\geq d(T_J)$, while the rest have dimension 1.

Step 4: The key inequality

Counting $\mathbb{F}_p$-dimensions using

$$V = \bigoplus_{i=1}^{m} g_i U, \qquad U = \bigotimes_{J} U_J, \qquad U_J = \bigotimes_{k=1}^{r(J)} U_{J,k},$$

we find

$$\dim V = m \dim U = m \prod_{J} \prod_{k=1}^{r(J)} \dim U_{J,k} \geq m \prod_{J} d(T_J)^{y(J)}.$$

Step 4: The key inequality

Counting $\mathbb{F}_p$-dimensions using

$$V = \bigoplus_{i=1}^{m} g_i U, \qquad U = \bigotimes_{J} U_J, \qquad U_J = \bigotimes_{k=1}^{r(J)} U_{J,k},$$

we find

$$\dim V = m \dim U = m \prod_{J} \prod_{k=1}^{r(J)} \dim U_{J,k} \geq m \prod_{J} d(T_J)^{y(J)}.$$

Since G acts transitively on V, we have $v_p(|G|) \geq \dim V$.

Step 4: The key inequality

Counting $\mathbb{F}_p$-dimensions using

$$V = \bigoplus_{i=1}^{m} g_i U, \qquad U = \bigotimes_{J} U_J, \qquad U_J = \bigotimes_{k=1}^{r(J)} U_{J,k},$$

we find

$$\dim V = m \dim U = m \prod_{J} \prod_{k=1}^{r(J)} \dim U_{J,k} \geq m \prod_{J} d(T_J)^{y(J)}.$$

Since G acts transitively on V, we have $v_p(|G|) \geq \dim V$.

Recall that $S = \mathrm{soc}(G)$ and $\mathrm{Cent}_G(S)$ is trivial. So G embeds in $\mathrm{Aut}(S)$.

Now S is the direct product of the minimal normal subgroups J, and each $J \cong T_J^{r(J)}$.

Now S is the direct product of the minimal normal subgroups J, and each $J \cong T_J^{r(J)}$.

Let $r = \sum_J r(J)$. Then S is the direct product of r non-abelian simple groups, and

$$G \leq \mathrm{Aut}(S) \leq \left(\prod_J \mathrm{Aut}(T_J)^{r(J)} \right) \rtimes S_r.$$

Now S is the direct product of the minimal normal subgroups J, and each $J \cong T_J^{r(J)}$.

Let $r = \sum_J r(J)$. Then S is the direct product of r non-abelian simple groups, and

$$G \leq \mathrm{Aut}(S) \leq \left(\prod_J \mathrm{Aut}(T_J)^{r(J)} \right) \rtimes S_r.$$

Hence

$$v_p(G) < \left(\sum_J r(J) v_p(|\mathrm{Aut}(T_J)|) \right) + \frac{r}{p-1}.$$

Now S is the direct product of the minimal normal subgroups J, and each $J \cong T_J^{r(J)}$.

Let $r = \sum_J r(J)$. Then S is the direct product of r non-abelian simple groups, and

$$G \leq \mathrm{Aut}(S) \leq \left(\prod_J \mathrm{Aut}(T_J)^{r(J)} \right) \rtimes S_r.$$

Hence

$$v_p(G) < \left(\sum_J r(J) v_p(|\mathrm{Aut}(T_J)|) \right) + \frac{r}{p-1}.$$

Combining with our lower bound on dim V, we get the Key Inequality

$$m \prod_J d(T_J)^{y(J)} < \sum_J r(J) \left(v_p(|\mathrm{Aut}(T_J)|) + \frac{1}{p-1} \right).$$

Step 5: Applying the Classification of Finite Simple Groups

Recall that each composition factor of G has a soluble subgroup of index p^s, $s \geq 0$.

Step 5: Applying the Classification of Finite Simple Groups

Recall that each composition factor of G has a soluble subgroup of index p^s, $s \geq 0$.

Using CFSG, Guralnick found all non-abelian simple groups with a proper subgroup of prime-power index. We can deduce from this:

Proposition:
If T is a non-abelian simple group with *soluble* subgroup of index p^a then (T, p, a) is one of:

(i) $(\mathrm{PSL}_3(2), 7, 1)$;

(ii) $(\mathrm{PSL}_3(3), 13, 1)$;

(iii) $(\mathrm{PSL}_2(2^a), p, 1)$ where $p = 2^a + 1 \geq 5$ is a Fermat prime;

(iv) $(\mathrm{PSL}_2(8), 3, 2)$;

(v) $(\mathrm{PSL}_2(q), 2, a)$ where $q = 2^a - 1 \geq 7$ is a Mersenne prime.

All these T have $|\mathrm{Out}(T)| = 2$. Note that $\mathrm{PSL}_3(2) = \mathrm{GL}_3(2) \cong \mathrm{PSL}_2(7)$ is the simple group of order 168.

If the Key Inequality

$$m \prod_J d(T_J)^{y(J)} < \sum_J r(J) \left(v_p(|\mathrm{Aut}(T_J)|) + \frac{1}{p-1} \right).$$

holds, then (replacing the product by a sum) we find that there must be at least one minimal normal subgroup J of G for which T_J satisfies

$$\frac{1}{y(J)} d(T_J)^{y(J)} < v_P(|\mathrm{Aut}(T_J)| + \frac{1}{p-1}. \qquad (1)$$

In cases (i)–(iii) of the Proposition, the trivial bound $d(T_J) \geq 2$ is enough to show this is impossible. In case (iv), where $p = 3$ and $T = \mathrm{PSL}_2(8)$, we need to know $d(T) = 7$.

So G has at least one composition factor of type (v): $T = \mathrm{PSL}_2(q)$ with $q = 2^a - 1 \geq 7$. Hence $p = 2$ and all non-abelian composition factors must be of this type (maybe for different q).

Now $d(T) = (q-1)/2$, and (1) is only satisfied for $a = 3$, i.e. $p = 7$, and $y(J) = 1$ or 2.

Hence $T_J = \mathrm{PSL}_2(7)$ for at least one J, and every T_J is of the form $\mathrm{PSL}_2(q)$. Putting this extra information into the Key Inequality, we can then show that only $q = 7$ works, so *every* non-abelian composition factor of G is $\mathrm{PSL}_2(7) \cong \mathrm{GL}_3(2)$.

This shows that

$$\mathrm{soc}(G) = \underbrace{\mathrm{GL}_3(2) \times \cdots \times \mathrm{GL}_3(2)}_{r}$$

for some $r \geq 1$. With a little extra work, we can check that

$$V = \underbrace{\mathbb{F}_2^3 \times \cdots \times \mathbb{F}_2^3}$$

with each copy of $\mathrm{GL}_3(2)$ acting on a single copy of $\mathbb{F}_2^3$, i.e. $y(J) = 1$. Moreover $G/\mathrm{soc}(G)$ is a transitive soluble subgroup of S_r.

So our irreducible pair (G, V) is as claimed earlier.

References

[B, 2022]: On insoluble transitive subgroups in the holomorph of a finite soluble group, arXiv:2205.13464v1 (2022).

[B, 2004]: Hopf-Galois structures on field extensions with simple Galois groups, Bull. London Math. Soc. 36 (2004), 23-–29.

[Crespo & Salguero, 2020]: Computation of Hopf Galois structures on low degree separable extensions and classification of those for degrees p^2 and $2p$. Publ. Mat 64 (2020), 121–141.

[Gorshkov & Nasybullov, 2021]: Finite skew braces with solvable additive group. J. Algebra 574 (2021), 172-183.

[Stefanello & Trappeniers, 2022]: On bi-skew braces and brace blocks, arxiv:2205.15073v1.

[Tsang & Qin, 2020]: On the solvability of regular subgroups in the holomorph of a finite solvable group, Internat. J. Algebra Comput. 30 (2020) 253–265.