Hopf-Galois Structures on Separable Field Extensions of Degree pq

Andrew Darlington

Definitions

Let L/K be a field extension.

Definitions

Let L/K be a field extension. A *K-Hopf algebra H* is a K-vector space equipped with five K-linear maps $\mu, \iota, \Delta, \epsilon, S$ (multiplication, unit, comultiplication, counit, antipode) such that $(H, \mu, \iota, \Delta, \epsilon)$ is a K-bialgebra.

Definitions

Let L/K be a field extension. A *K-Hopf algebra* H is a K-vector space equipped with five K-linear maps $\mu, \iota, \Delta, \epsilon, S$ (multiplication, unit, comultiplication, counit, antipode) such that $(H, \mu, \iota, \Delta, \epsilon)$ is a K-bialgebra.

We say that H gives a *Hopf-Galois structure* on L/K if:

Definitions

Let L/K be a field extension. A *K-Hopf algebra* H is a K-vector space equipped with five K-linear maps $\mu, \iota, \Delta, \epsilon, S$ (multiplication, unit, comultiplication, counit, antipode) such that $(H, \mu, \iota, \Delta, \epsilon)$ is a K-bialgebra.

We say that H gives a *Hopf-Galois structure* on L/K if: H acts on L such that $\forall h \in H \; x, y \in L$,

$$\Delta(h) \cdot (x \otimes y) = \sum_{(h)} (h_{(1)} \cdot x) \otimes (h_{(2)} \cdot y)$$

Definitions

Let L/K be a field extension. A *K-Hopf algebra* H is a K-vector space equipped with five K-linear maps $\mu, \iota, \Delta, \epsilon, S$ (multiplication, unit, comultiplication, counit, antipode) such that $(H, \mu, \iota, \Delta, \epsilon)$ is a K-bialgebra.

We say that H gives a *Hopf-Galois structure* on L/K if: H acts on L such that $\forall h \in H$ $x, y \in L$,

$$\Delta(h) \cdot (x \otimes y) = \sum_{(h)} (h_{(1)} \cdot x) \otimes (h_{(2)} \cdot y)$$

and the K-linear map $\theta : L \otimes L \to \mathrm{Hom}(H, L)$, $\theta(x \otimes y)(h) = x(h \cdot y)$ is bijective.

Definitions

Let L/K be a field extension. A *K-Hopf algebra* H is a K-vector space equipped with five K-linear maps $\mu, \iota, \Delta, \epsilon, S$ (multiplication, unit, comultiplication, counit, antipode) such that $(H, \mu, \iota, \Delta, \epsilon)$ is a K-bialgebra.
We say that H gives a *Hopf-Galois structure* on L/K if: H acts on L such that $\forall h \in H$ $x, y \in L$,

$$\Delta(h) \cdot (x \otimes y) = \sum_{(h)} (h_{(1)} \cdot x) \otimes (h_{(2)} \cdot y)$$

and the K-linear map $\theta : L \otimes L \to \mathrm{Hom}(H, L)$, $\theta(x \otimes y)(h) = x(h \cdot y)$ is bijective.
The classic example of a Hopf-Galois structure on a Galois extension with Galois group G is that given by the group-algebra $K[G]$.

Byott's translation

L/K be a finite separable field extension. E the normal closure of L/K, $G = \mathrm{Gal}(E/K)$, $G' = \mathrm{Gal}(E/L)$, and $X = G/G'$.

Byott's translation

L/K be a finite separable field extension. E the normal closure of L/K, $G = \mathrm{Gal}(E/K)$, $G' = \mathrm{Gal}(E/L)$, and $X = G/G'$.
Then (by Greither & Pareigis [GP87]) there is a bijective correspondence between Hopf-Galois structures H on L/K, and regular subgroups N of $\mathrm{Perm}(X)$ normalised by the image of the left translations $\lambda(G)$: $H = E[N]^G$.

Byott's translation

L/K be a finite separable field extension. E the normal closure of L/K, $G = \mathrm{Gal}(E/K)$, $G' = \mathrm{Gal}(E/L)$, and $X = G/G'$.
Then (by Greither & Pareigis [GP87]) there is a bijective correspondence between Hopf-Galois structures H on L/K, and regular subgroups N of $\mathrm{Perm}(X)$ normalised by the image of the left translations $\lambda(G)$:
$H = E[N]^G$.
We say that the abstract isomorphism type of N is the *type* of the Hopf-Galois structure.

Byott's translation

L/K be a finite separable field extension. E the normal closure of L/K, $G = \mathrm{Gal}(E/K)$, $G' = \mathrm{Gal}(E/L)$, and $X = G/G'$.
Then (by Greither & Pareigis [GP87]) there is a bijective correspondence between Hopf-Galois structures H on L/K, and regular subgroups N of $\mathrm{Perm}(X)$ normalised by the image of the left translations $\lambda(G)$:
$H = E[N]^G$.
We say that the abstract isomorphism type of N is the *type* of the Hopf-Galois structure.

Theorem 1.1 (Byott 1996)

There is a bijection between

$$\mathcal{N} = \{\alpha : N \to Perm(X) \mid \alpha \text{ inj. hom. s.t. } \alpha(N) \text{ is regular}\}, \text{ and}$$
$$\mathcal{G} = \left\{\beta : G \to Perm(N) \mid \beta \text{ inj. hom. s.t. } \beta(G') = Stab(1_N)\right\}.$$

$\alpha(N)$ is normalised by $\lambda(G)$ iff $\beta(G)$ is contained in $Hol(N)$.

Counting formula

Lemma 1.2 (Byott 1996)

Let $e(G,N) = \#HGS$ *of type* N *which realise* G*,*

$$e'(G,N) = \left| \left\{ M < Hol(N) \text{ transitive } \mid M \overset{\phi}{\cong} G \text{ s.t. } \phi(Stab_M(1_N)) = G' \right\} \right|.$$

Then

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

$$\mathrm{Aut}(G,G') = \left\{ \theta \in \mathrm{Aut}(G) \mid \theta(G') = G' \right\}.$$

Strategy

The strategy of categorising and counting Hopf-Galois structures becomes:

Strategy

The strategy of categorising and counting Hopf-Galois structures becomes:

- Give a characterisation for the groups N we want to study.

Strategy

The strategy of categorising and counting Hopf-Galois structures becomes:

- Give a characterisation for the groups N we want to study.
- For each N, compute the transitive subgroups G of $\mathrm{Hol}(N)$ (NB: for a Galois extension, $|G| = |N|$, so look at regular subgroups).

Strategy

The strategy of categorising and counting Hopf-Galois structures becomes:

- Give a characterisation for the groups N we want to study.
- For each N, compute the transitive subgroups G of $\mathrm{Hol}(N)$ (NB: for a Galois extension, $|G| = |N|$, so look at regular subgroups).
- Determine which G are isomorphic as permutation groups (that is, for two such groups G_1, G_2, there is an isomorphism between them which takes $\mathrm{Stab}_{G_1}(1_N)$ to $\mathrm{Stab}_{G_2}(1_N)$).

Strategy

The strategy of categorising and counting Hopf-Galois structures becomes:

- Give a characterisation for the groups N we want to study.
- For each N, compute the transitive subgroups G of $\mathrm{Hol}(N)$ (NB: for a Galois extension, $|G| = |N|$, so look at regular subgroups).
- Determine which G are isomorphic as permutation groups (that is, for two such groups G_1, G_2, there is an isomorphism between them which takes $\mathrm{Stab}_{G_1}(1_N)$ to $\mathrm{Stab}_{G_2}(1_N)$).
- Compute $\mathrm{Aut}(G, G')$ in each case, and use Lemma 1.2 to count the number of Hopf-Galois structures of type N which realise G.

Strategy

The strategy of categorising and counting Hopf-Galois structures becomes:

- Give a characterisation for the groups N we want to study.
- For each N, compute the transitive subgroups G of $\mathrm{Hol}(N)$ (NB: for a Galois extension, $|G| = |N|$, so look at regular subgroups).
- Determine which G are isomorphic as permutation groups (that is, for two such groups G_1, G_2, there is an isomorphism between them which takes $\mathrm{Stab}_{G_1}(1_N)$ to $\mathrm{Stab}_{G_2}(1_N)$).
- Compute $\mathrm{Aut}(G, G')$ in each case, and use Lemma 1.2 to count the number of Hopf-Galois structures of type N which realise G.
- Suppose one finds a $G_1 < \mathrm{Hol}(N_1)$ and a $G_2 < \mathrm{Hol}(N_2)$ with $G_1 \cong G_2$, then we see that $G_1 \cong G_2$ admits Hopf-Galois structures of types N_1 and N_2.

Squarefree extensions

We look at separable (but not necessarily normal) field extensions of squarefree degree.

Squarefree extensions

We look at separable (but not necessarily normal) field extensions of squarefree degree.

- Part I: extensions of degree pq where p, q distinct odd primes.

Squarefree extensions

We look at separable (but not necessarily normal) field extensions of squarefree degree.

- Part I: extensions of degree pq where p, q distinct odd primes.
- Part II: other degree pq extensions.

Squarefree extensions

We look at separable (but not necessarily normal) field extensions of squarefree degree.

- Part I: extensions of degree pq where p, q distinct odd primes.
- Part II: other degree pq extensions.
- Part III: more general squarefree extensions

Squarefree extensions

We look at separable (but not necessarily normal) field extensions of squarefree degree.

- Part I: extensions of degree pq where p, q distinct odd primes.
- Part II: other degree pq extensions.
- Part III: more general squarefree extensions
    - Part IIIa: extensions of degree pqr where p, q, r distinct odd primes.

Squarefree extensions

We look at separable (but not necessarily normal) field extensions of squarefree degree.

- Part I: extensions of degree pq where p, q distinct odd primes.
- Part II: other degree pq extensions.
- Part III: more general squarefree extensions
  - Part IIIa: extensions of degree pqr where p, q, r distinct odd primes.
  - Part IIIb: extensions of degree $n = p_1 \cdots p_m$ where $p_i = 2p_{i+1} + 1$.

Squarefree extensions

We look at separable (but not necessarily normal) field extensions of squarefree degree.

- Part I: extensions of degree pq where p, q distinct odd primes.
- Part II: other degree pq extensions.
- Part III: more general squarefree extensions
  - Part IIIa: extensions of degree pqr where p, q, r distinct odd primes.
  - Part IIIb: extensions of degree $n = p_1 \cdots p_m$ where $p_i = 2p_{i+1} + 1$.
  - Part IIIc: what's next?

Remark 1.3

- *Byott & Alabdali [AB20] looked at Galois extensions of squarefree degree.*

Remark 1.3

- Byott & Alabdali [AB20] looked at Galois extensions of squarefree degree.
- Byott & Martin-Lyons [BML22] looked at separable extensions of degree pq with $p = 2q + 1$ (q is a Sophie Germain prime and p is a safe prime) - this was talked about in last year's conference.

Remark 1.3

- *Byott & Alabdali [AB20] looked at Galois extensions of squarefree degree.*
- *Byott & Martin-Lyons [BML22] looked at separable extensions of degree pq with $p = 2q + 1$ (q is a Sophie Germain prime and p is a safe prime) - this was talked about in last year's conference.*
- *This talk extends that theory.*

Remark 1.3

- Byott & Alabdali [AB20] looked at Galois extensions of squarefree degree.
- Byott & Martin-Lyons [BML22] looked at separable extensions of degree pq with $p = 2q + 1$ (q is a Sophie Germain prime and p is a safe prime) - this was talked about in last year's conference.
- This talk extends that theory.- The work of Crespo & Salguero in [CS20] which looks at degree p^2 and $2p$ completes the product of two primes discussion.

Remark 1.3

- Byott & Alabdali [AB20] looked at Galois extensions of squarefree degree.
- Byott & Martin-Lyons [BML22] looked at separable extensions of degree pq with $p = 2q + 1$ (q is a Sophie Germain prime and p is a safe prime) - this was talked about in last year's conference.
- This talk extends that theory.- The work of Crespo & Salguero in [CS20] which looks at degree p^2 and $2p$ completes the product of two primes discussion.

An abstract group of order pq has presentation:

$$N \cong \langle \sigma, \tau \mid \sigma^p = \tau^q = 1, \tau\sigma\tau^{-1} = \sigma^k \rangle$$

where k is either 1 or has order $q \mod p$, giving the two groups C_{pq} and $C_p \rtimes C_q$.

Remark 1.3

- Byott & Alabdali [AB20] looked at Galois extensions of squarefree degree.
- Byott & Martin-Lyons [BML22] looked at separable extensions of degree pq with $p = 2q + 1$ (q is a Sophie Germain prime and p is a safe prime) - this was talked about in last year's conference.
- This talk extends that theory.- The work of Crespo & Salguero in [CS20] which looks at degree p^2 and $2p$ completes the product of two primes discussion.

An abstract group of order pq has presentation:

$$N \cong \langle \sigma, \tau \mid \sigma^p = \tau^q = 1, \tau\sigma\tau^{-1} = \sigma^k \rangle$$

where k is either 1 or has order $q \mod p$, giving the two groups C_{pq} and $C_p \rtimes C_q$.

Cyclic case

Let $N \cong C_{pq}$ and:

$$p - 1 = q^{e_0} \ell_1^{e_1} \cdots \ell_m^{e_m},$$
$$q - 1 = \ell_1^{f_1} \cdots \ell_m^{f_m},$$

$e_0 > 0, e_i, f_i \geq 0$ for $1 \leq i \leq m$, and $\max\{e_m, f_m\} > 0$.

Cyclic case

Let $N \cong C_{pq}$ and:

$$p - 1 = q^{e_0} \ell_1^{e_1} \cdots \ell_m^{e_m},$$
$$q - 1 = \ell_1^{f_1} \cdots \ell_m^{f_m},$$

$e_0 > 0, e_i, f_i \geq 0$ for $1 \leq i \leq m$, and $\max\{e_m, f_m\} > 0$.
$\mathrm{Aut}(N) \cong \mathrm{Aut}(\langle\sigma\rangle) \times \mathrm{Aut}(\langle\tau\rangle)$ is generated by the following elements:

Cyclic case

Let $N \cong C_{pq}$ and:

$$p - 1 = q^{e_0} \ell_1^{e_1} \cdots \ell_m^{e_m},$$
$$q - 1 = \ell_1^{f_1} \cdots \ell_m^{f_m},$$

$e_0 > 0, e_i, f_i \geq 0$ for $1 \leq i \leq m$, and $\max\{e_m, f_m\} > 0$.
$\mathrm{Aut}(N) \cong \mathrm{Aut}(\langle\sigma\rangle) \times \mathrm{Aut}(\langle\tau\rangle)$ is generated by the following elements:

$$\alpha \in \mathrm{Aut}(\langle\sigma\rangle) \text{ s.t. } \mathrm{ord}(\alpha) = q^{e_0},$$
$$\alpha_i \in \mathrm{Aut}(\langle\sigma\rangle) \text{ s.t. } \mathrm{ord}(\alpha_i) = \ell_i^{e_i},$$
$$\beta_i \in \mathrm{Aut}(\langle\tau\rangle) \text{ s.t. } \mathrm{ord}(\beta_i) = \ell_i^{f_i},$$

Cyclic case

Let $N \cong C_{pq}$ and:

$$p - 1 = q^{e_0} \ell_1^{e_1} \cdots \ell_m^{e_m},$$
$$q - 1 = \ell_1^{f_1} \cdots \ell_m^{f_m},$$

$e_0 > 0, e_i, f_i \geq 0$ for $1 \leq i \leq m$, and $\max\{e_m, f_m\} > 0$.
$\mathrm{Aut}(N) \cong \mathrm{Aut}(\langle\sigma\rangle) \times \mathrm{Aut}(\langle\tau\rangle)$ is generated by the following elements:

$$\alpha \in \mathrm{Aut}(\langle\sigma\rangle) \text{ s.t. } \mathrm{ord}(\alpha) = q^{e_0},$$
$$\alpha_i \in \mathrm{Aut}(\langle\sigma\rangle) \text{ s.t. } \mathrm{ord}(\alpha_i) = \ell_i^{e_i},$$
$$\beta_i \in \mathrm{Aut}(\langle\tau\rangle) \text{ s.t. } \mathrm{ord}(\beta_i) = \ell_i^{f_i},$$

$$\mathrm{Aut}(N) \cong \langle\alpha\rangle \times \langle\alpha_1, \beta_1\rangle \times \cdots \times \langle\alpha_m, \beta_m\rangle.$$

Transitive subgroups of the unique Hall $\{p, q\}$-subgroup $H = \langle \sigma, \tau, \alpha \rangle$:

Transitive subgroups of the unique Hall $\{p, q\}$-subgroup $H = \langle \sigma, \tau, \alpha \rangle$:

$$N,$$

Transitive subgroups of the unique Hall $\{p, q\}$-subgroup $H = \langle \sigma, \tau, \alpha \rangle$:

$$N,$$

$$H,$$

Transitive subgroups of the unique Hall $\{p, q\}$-subgroup $H = \langle \sigma, \tau, \alpha \rangle$:

$$N,$$

$$H,$$

$$J_{t,c_0} := \left\langle \sigma, \left[\tau, \alpha^{q^{e_0 - c_0} t} \right] \right\rangle .$$

Transitive subgroups of the unique Hall $\{p, q\}$-subgroup $H = \langle \sigma, \tau, \alpha \rangle$:

$$N,$$

$$H,$$

$$J_{t,c_0} := \left\langle \sigma, \left[\tau, \alpha^{q^{e_0 - c_0} t} \right] \right\rangle.$$

Every transitive subgroup of Hol(N) **must** contain either N or some J_{t,c_0};

Transitive subgroups of the unique Hall $\{p, q\}$-subgroup $H = \langle \sigma, \tau, \alpha \rangle$:

$$N,$$

$$H,$$

$$J_{t,c_0} := \left\langle \sigma, \left[\tau, \alpha^{q^{e_0 - c_0} t} \right] \right\rangle .$$

Every transitive subgroup of $\mathrm{Hol}(N)$ **must** contain either N or some J_{t,c_0}; N is normalised by $\mathrm{Aut}(N)$; J_{t,c_0} is normalised by $\mathrm{Aut}(\langle \sigma \rangle)$. So any transitive subgroup of $\mathrm{Hol}(N)$ has of one of the following two forms:

Transitive subgroups of the unique Hall $\{p, q\}$-subgroup $H = \langle \sigma, \tau, \alpha \rangle$:

$$N,$$

$$H,$$

$$J_{t,c_0} := \left\langle \sigma, \left[\tau, \alpha^{q^{e_0 - c_0} t}\right] \right\rangle.$$

Every transitive subgroup of $\mathrm{Hol}(N)$ **must** contain either N or some J_{t,c_0}; N is normalised by $\mathrm{Aut}(N)$; J_{t,c_0} is normalised by $\mathrm{Aut}(\langle \sigma \rangle)$. So any transitive subgroup of $\mathrm{Hol}(N)$ has of one of the following two forms:

$$N \rtimes A, \ A \text{ any subgroup of } \mathrm{Aut}(N)$$
$$J_{t,c_0} \rtimes B, \ B \text{ any subgroup of } \mathrm{Aut}(\langle \sigma \rangle)$$

Subgroups of Aut($\langle\sigma\rangle$): $\left\langle \alpha^{q^{e_0-c_0}t_0}, \alpha_1^{\ell_1^{e_1-c_1}t_1}, \cdots, \alpha_m^{\ell_m^{e_m-c_m}t_m} \right\rangle$.

Subgroups of Aut($\langle\sigma\rangle$): $\left\langle \alpha^{q^{e_0-c_0}t_0}, \alpha_1^{\ell_1^{e_1-c_1}t_1}, \cdots, \alpha_m^{\ell_m^{e_m-c_m}t_m} \right\rangle$. Subgroups of Aut($N$) are of the form $A_0 \times A_1 \times \cdots \times A_m$ where $A_0 < \langle\alpha\rangle$, and $A_i < \langle\alpha_i, \beta_i\rangle$.

Subgroups of $\mathrm{Aut}(\langle\sigma\rangle)$: $\left\langle \alpha^{q^{e_0-c_0}t_0}, \alpha_1^{\ell_1^{e_1-c_1}t_1}, \cdots, \alpha_m^{\ell_m^{e_m-c_m}t_m} \right\rangle$. Subgroups of $\mathrm{Aut}(N)$ are of the form $A_0 \times A_1 \times \cdots \times A_m$ where $A_0 < \langle\alpha\rangle$, and $A_i < \langle\alpha_i, \beta_i\rangle$.

Lemma 2.1

The subgroups of $\langle\alpha_i, \beta_i\rangle$ are as follows:

Subgroups of $\mathrm{Aut}(\langle\sigma\rangle)$: $\left\langle \alpha^{q^{e_0-c_0}t_0}, \alpha_1^{\ell_1^{e_1-c_1}t_1}, \cdots, \alpha_m^{\ell_m^{e_m-c_m}t_m} \right\rangle$. Subgroups of $\mathrm{Aut}(N)$ are of the form $A_0 \times A_1 \times \cdots \times A_m$ where $A_0 < \langle\alpha\rangle$, and $A_i < \langle\alpha_i, \beta_i\rangle$.

Lemma 2.1

The subgroups of $\langle\alpha_i, \beta_i\rangle$ are as follows:

$$\text{(i)} \left\langle \alpha_i^{\ell_i^{e_i-c_{i_1}}}, \beta_i^{\ell_i^{f_i-d_{i_2}}} \right\rangle,$$

Subgroups of $\mathrm{Aut}(\langle\sigma\rangle)$: $\left\langle \alpha^{q^{e_0-c_0}t_0}, \alpha_1^{\ell_1^{e_1-c_1}t_1}, \cdots, \alpha_m^{\ell_m^{e_m-c_m}t_m} \right\rangle$. Subgroups of $\mathrm{Aut}(N)$ are of the form $A_0 \times A_1 \times \cdots \times A_m$ where $A_0 < \langle\alpha\rangle$, and $A_i < \langle\alpha_i, \beta_i\rangle$.

Lemma 2.1

The subgroups of $\langle\alpha_i, \beta_i\rangle$ are as follows:

$$\text{(i)} \left\langle \alpha_i^{\ell_i^{e_i-c_{i_1}}}, \beta_i^{\ell_i^{f_i-d_{i_2}}} \right\rangle,$$
$$\text{(ii)} \left\langle \alpha_i^{n_i\ell_i^{e_i-c_{i_1}}} \beta_i^{\ell_i^{f_i-d_{i_1}}} \right\rangle,$$

Subgroups of $\mathrm{Aut}(\langle\sigma\rangle)$: $\left\langle \alpha^{q^{e_0-c_0}t_0}, \alpha_1^{\ell_1^{e_1-c_1}t_1}, \cdots, \alpha_m^{\ell_m^{e_m-c_m}t_m} \right\rangle$. Subgroups of $\mathrm{Aut}(N)$ are of the form $A_0 \times A_1 \times \cdots \times A_m$ where $A_0 < \langle\alpha\rangle$, and $A_i < \langle \alpha_i, \beta_i \rangle$.

Lemma 2.1

The subgroups of $\langle \alpha_i, \beta_i \rangle$ *are as follows:*

$$\text{(i)} \left\langle \alpha_i^{\ell_i^{e_i-c_{i_1}}}, \beta_i^{\ell_i^{f_i-d_{i_2}}} \right\rangle,$$

$$\text{(ii)} \left\langle \alpha_i^{n_i\ell_i^{e_i-c_{i_1}}} \beta_i^{\ell_i^{f_i-d_{i_1}}} \right\rangle,$$

$$\text{(iii)} \left\langle \alpha_i^{n_i\ell_i^{e_i-c_{i_1}}} \beta_i^{\ell_i^{f_i-d_{i_1}}}, \beta_i^{\ell_i^{f_i-d_{i_2}}} \right\rangle.$$

Subgroups of $\mathrm{Aut}(\langle\sigma\rangle)$: $\left\langle \alpha^{q^{e_0-c_0}t_0}, \alpha_1^{\ell_1^{e_1-c_1}t_1}, \cdots, \alpha_m^{\ell_m^{e_m-c_m}t_m} \right\rangle$. Subgroups of $\mathrm{Aut}(N)$ are of the form $A_0 \times A_1 \times \cdots \times A_m$ where $A_0 < \langle\alpha\rangle$, and $A_i < \langle \alpha_i, \beta_i \rangle$.

Lemma 2.1

The subgroups of $\langle \alpha_i, \beta_i \rangle$ are as follows:

$$\text{(i)} \left\langle \alpha_i^{\ell_i^{e_i-c_{i_1}}}, \beta_i^{\ell_i^{f_i-d_{i_2}}} \right\rangle,$$
$$\text{(ii)} \left\langle \alpha_i^{n_i\ell_i^{e_i-c_{i_1}}} \beta_i^{\ell_i^{f_i-d_{i_1}}} \right\rangle,$$
$$\text{(iii)} \left\langle \alpha_i^{n_i\ell_i^{e_i-c_{i_1}}} \beta_i^{\ell_i^{f_i-d_{i_1}}}, \beta_i^{\ell_i^{f_i-d_{i_2}}} \right\rangle.$$

Conditions on indices omitted.

Lemma 2.2 (isomorphisms)

Let $A, A' < Aut(N)$ *and* $B, B' < Aut(\langle \sigma \rangle)$.

Lemma 2.2 (isomorphisms)

Let $A, A' < Aut(N)$ *and* $B, B' < Aut(\langle\sigma\rangle)$. *Then*

$$N \rtimes A \cong N \rtimes A' \implies A = A'$$

and

$$J_{t,c_0} \rtimes B \cong J_{t,c_0} \rtimes B' \implies B = B'.$$

Lemma 2.2 (isomorphisms)

Let $A, A' < Aut(N)$ *and* $B, B' < Aut(\langle\sigma\rangle)$. *Then*

$$N \rtimes A \cong N \rtimes A' \implies A = A'$$

and

$$J_{t,c_0} \rtimes B \cong J_{t,c_0} \rtimes B' \implies B = B'.$$

Further, we have that $J_{t,c_0} \cong J_{t',c_0}\ \forall t, t'$ *coprime to* q.

Lemma 2.2 (isomorphisms)

Let $A, A' < Aut(N)$ *and* $B, B' < Aut(\langle\sigma\rangle)$. *Then*

$$N \rtimes A \cong N \rtimes A' \implies A = A'$$

and

$$J_{t,c_0} \rtimes B \cong J_{t,c_0} \rtimes B' \implies B = B'.$$

Further, we have that $J_{t,c_0} \cong J_{t',c_0}$ $\forall t, t'$ *coprime to* q.

Theorem 2.3

For groups of type $N \rtimes A$ *for some* $A < Aut(N)$, *or of type* $J_{t,c_0} \rtimes B$ *for some* $B \neq \{1\}$, *there is a unique Hopf-Galois structure of cyclic type.*

Lemma 2.2 (isomorphisms)

Let $A, A' < Aut(N)$ *and* $B, B' < Aut(\langle\sigma\rangle)$. *Then*

$$N \rtimes A \cong N \rtimes A' \implies A = A'$$

and

$$J_{t,c_0} \rtimes B \cong J_{t,c_0} \rtimes B' \implies B = B'.$$

Further, we have that $J_{t,c_0} \cong J_{t',c_0}$ $\forall t, t'$ *coprime to* q.

Theorem 2.3

For groups of type $N \rtimes A$ *for some* $A < Aut(N)$, *or of type* $J_{t,c_0} \rtimes B$ *for some* $B \neq \{1\}$, *there is a unique Hopf-Galois structure of cyclic type.* *For groups of type* J_{t,c_0}, *there are* p *Hopf-Galois structures of cyclic type.*

Lemma 2.2 (isomorphisms)

Let $A, A' < Aut(N)$ *and* $B, B' < Aut(\langle\sigma\rangle)$. *Then*

$$N \rtimes A \cong N \rtimes A' \implies A = A'$$

and

$$J_{t,c_0} \rtimes B \cong J_{t,c_0} \rtimes B' \implies B = B'.$$

Further, we have that $J_{t,c_0} \cong J_{t',c_0}$ $\forall t, t'$ *coprime to* q.

Theorem 2.3

For groups of type $N \rtimes A$ *for some* $A < Aut(N)$, *or of type* $J_{t,c_0} \rtimes B$ *for some* $B \neq \{1\}$, *there is a unique Hopf-Galois structure of cyclic type. For groups of type* J_{t,c_0}, *there are* p *Hopf-Galois structures of cyclic type.*

$$G \cong ((C_p \rtimes C_{q^{c_0} d_1}) \times (C_q \rtimes C_{d_2})) \rtimes C_{d_3}$$

where d_1, d_2, d_3 are some divisors of $\varphi(n)$ coprime to n.

We have, in total:

$$(1+e_0)\prod_{1\le i\le m}\left[(e_i+1)(f_i+1)+f_i(\ell_i^{e_i}-1)+\Sigma_i\right]+e_0\prod_{1\le i\le m}(e_i+1)$$

isomorphism types of permutation groups G of degree pq which are realised by a Hopf-Galois structure of cyclic type. (Σ_i gives a count of the number of subgroups of $\langle\alpha_i,\beta_i\rangle$ of type (iii), formula omitted).

Remark 2.4

Setting $e_0=1$, $\ell_1=2$, $e_1=1$, $f_1=r$, $s=\ell_2^{f_2}\cdots\ell_m^{f_m}$, $e_i=0$ for $2\le i\le n$, and noting that $\Sigma_i=0$ for $1\le i\le n$, we retrieve the result of Byott and Martin-Lyons that there are

$$(6r+4)\prod_{2\le i\le n}(f_i+1)+2=(6r+4)\sigma_0(s)+2$$

($\sigma_0(s)$ counts the number of divisors of s) isomorphism types of permutation groups G of degree pq (with $p=2q+1$ a Sophie Germain prime pair) which are realised by a Hopf-Galois structure of cyclic type.

Metabelian case

Let $N \cong C_p \rtimes C_q$. $\mathrm{Aut}(N)$ has order $p(p-1) = pq^{e_0}s$ where $s \mid p-1$ coprime to q, and is generated by α, β, ϵ of orders q^{e_0}, s, p respectively such that

$$\alpha(\sigma) = \sigma^{a_\alpha}, \qquad \alpha(\tau) = \tau,$$
$$\beta(\sigma) = \sigma^{a_\beta}, \qquad \beta(\tau) = \tau,$$
$$\epsilon(\sigma) = \sigma, \qquad \epsilon(\tau) = \sigma\tau.$$

Metabelian case

Let $N \cong C_p \rtimes C_q$. $\mathrm{Aut}(N)$ has order $p(p-1) = pq^{e_0}s$ where $s \mid p-1$ coprime to q, and is generated by α, β, ϵ of orders q^{e_0}, s, p respectively such that

$$\begin{aligned} \alpha(\sigma) &= \sigma^{a_\alpha}, & \alpha(\tau) &= \tau, \\ \beta(\sigma) &= \sigma^{a_\beta}, & \beta(\tau) &= \tau, \\ \epsilon(\sigma) &= \sigma, & \epsilon(\tau) &= \sigma\tau. \end{aligned}$$

$|\mathrm{Hol}(N)| = p^2 q^{e_0+1} s$

Metabelian case

Let $N \cong C_p \rtimes C_q$. Aut(N) has order $p(p-1) = pq^{e_0}s$ where $s \mid p-1$ coprime to q, and is generated by α, β, ϵ of orders q^{e_0}, s, p respectively such that

$$\begin{aligned} \alpha(\sigma) &= \sigma^{a_\alpha}, & \alpha(\tau) &= \tau, \\ \beta(\sigma) &= \sigma^{a_\beta}, & \beta(\tau) &= \tau, \\ \epsilon(\sigma) &= \sigma, & \epsilon(\tau) &= \sigma\tau. \end{aligned}$$

$|\mathrm{Hol}(N)| = p^2 q^{e_0+1} s$
Idea: $(\sigma\epsilon^{k-1})\tau = \tau(\sigma\epsilon^{k-1})$, so:

Metabelian case

Let $N \cong C_p \rtimes C_q$. $\mathrm{Aut}(N)$ has order $p(p-1) = pq^{e_0}s$ where $s \mid p-1$ coprime to q, and is generated by α, β, ϵ of orders q^{e_0}, s, p respectively such that

$$\begin{aligned} \alpha(\sigma) &= \sigma^{a_\alpha}, & \alpha(\tau) &= \tau, \\ \beta(\sigma) &= \sigma^{a_\beta}, & \beta(\tau) &= \tau, \\ \epsilon(\sigma) &= \sigma, & \epsilon(\tau) &= \sigma\tau. \end{aligned}$$

$|\mathrm{Hol}(N)| = p^2 q^{e_0+1} s$
Idea: $(\sigma\epsilon^{k-1})\tau = \tau(\sigma\epsilon^{k-1})$, so:

$$\mathrm{Hol}(N) = \langle \sigma, \tau \rangle \rtimes \langle \alpha, \beta, \epsilon \rangle \cong \langle \sigma, \sigma\epsilon^{k-1} \rangle \rtimes \langle \tau, \alpha, \beta \rangle \cong \mathbb{F}_p^2 \rtimes \langle T, A, B \rangle.$$

Metabelian case

Let $N \cong C_p \rtimes C_q$. $\mathrm{Aut}(N)$ has order $p(p-1) = pq^{e_0}s$ where $s \mid p-1$ coprime to q, and is generated by α, β, ϵ of orders q^{e_0}, s, p respectively such that

$$\begin{aligned} \alpha(\sigma) &= \sigma^{a_\alpha}, & \alpha(\tau) &= \tau, \\ \beta(\sigma) &= \sigma^{a_\beta}, & \beta(\tau) &= \tau, \\ \epsilon(\sigma) &= \sigma, & \epsilon(\tau) &= \sigma\tau. \end{aligned}$$

$|\mathrm{Hol}(N)| = p^2 q^{e_0+1} s$
Idea: $(\sigma\epsilon^{k-1})\tau = \tau(\sigma\epsilon^{k-1})$, so:

$$\mathrm{Hol}(N) = \langle \sigma, \tau \rangle \rtimes \langle \alpha, \beta, \epsilon \rangle \cong \langle \sigma, \sigma\epsilon^{k-1} \rangle \rtimes \langle \tau, \alpha, \beta \rangle \cong \mathbb{F}_p^2 \rtimes \langle T, A, B \rangle.$$

$$T = \begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix}, \qquad A = \begin{pmatrix} a_\alpha & 0 \\ 0 & a_\alpha \end{pmatrix}, \qquad B = \begin{pmatrix} a_\beta & 0 \\ 0 & a_\beta \end{pmatrix}$$

Identify $\mathbb{F}_p^2 = \langle \mathbf{e}_1, \mathbf{e}_2 \rangle$ with $\langle \sigma, \sigma\epsilon^{k-1} \rangle$.

Identify $\mathbb{F}_p^2 = \langle \mathbf{e}_1, \mathbf{e}_2 \rangle$ with $\langle \sigma, \sigma\epsilon^{k-1} \rangle$.

Lemma 2.5

A subgroup M of $Hol(N)$ is transitive on N if and only if it satisfies the following two conditions:

Identify $\mathbb{F}_p^2 = \langle \mathbf{e}_1, \mathbf{e}_2 \rangle$ with $\langle \sigma, \sigma\epsilon^{k-1} \rangle$.

Lemma 2.5

A subgroup M of $Hol(N)$ is transitive on N if and only if it satisfies the following two conditions:

(i) the image of M under the quotient map $Hol(N) \to \langle T, A, B \rangle$ is one of

$$\left\langle TA^{uq^{e_0-c_0}}, B^{s/d} \right\rangle, \ u \in (\mathbb{Z}/q^{c_0}\mathbb{Z})^\times, \ 0 \le c_0 \le e_0, \ d|s,$$

$$\left\langle T, A^{q^{e_0-c_0}}, B^{s/d} \right\rangle, \ 1 \le c_0 \le e_0, \ d|s.$$

(ii) $M \cap P$ is one of $\mathbb{F}_p^2$, $\mathbb{F}_p\mathbf{e}_1$, $\mathbb{F}_p\mathbf{e}_2$, each of which is normalised by $\langle T, A, B \rangle$.

Lemma 1

The transitive subgroups of order divisible by p^2q *are:*

(i) $P \rtimes \left\langle TA^{uq^{e_0-c_0}}, B^{s/d} \right\rangle$, $u \in (\mathbb{Z}/q^{c_0}\mathbb{Z})^\times$, $0 \leq c_0 \leq e_0$, $d|s$. *These groups have order* $dp^2q^{\max\{1,c_0\}}$.

(ii) $P \rtimes \left\langle T, A^{q^{e_0-c_0}}, B^{s/d} \right\rangle$, $1 \leq c_0 \leq e_0$, $d|s$. *These groups have order* $dp^2q^{1+c_0}$.

Lemma 1

The transitive subgroups of order divisible by $p^2 q$ *are:*

(i) $P \rtimes \left\langle TA^{uq^{e_0-c_0}}, B^{s/d} \right\rangle$, $u \in (\mathbb{Z}/q^{c_0}\mathbb{Z})^\times$, $0 \leq c_0 \leq e_0$, $d|s$. *These groups have order* $dp^2 q^{\max\{1,c_0\}}$.

(ii) $P \rtimes \left\langle T, A^{q^{e_0-c_0}}, B^{s/d} \right\rangle$, $1 \leq c_0 \leq e_0$, $d|s$. *These groups have order* $dp^2 q^{1+c_0}$.

Now suppose $p^2 \nmid |M|$, we have that, for some $0 \leq c_0 \leq e_0$, $u \in (\mathbb{Z}/q^{c_0}\mathbb{Z})^\times$, $d \mid s$, and $\lambda, \mu, \nu \in \mathbb{F}_p$, M is generated by the set:

(I) $\left\{ \mathbf{e}_i, [\lambda \mathbf{e}_i, TA^{uq^{e_0-c_0}}], [\mu \mathbf{e}_i, B^{s/d}] \right\}$, or the set

(II) $\left\{ \mathbf{e}_i, [\lambda \mathbf{e}_i, T], [\mu \mathbf{e}_i, A^{q^{e_0-c_0}}], [\nu \mathbf{e}_i, B^{s/d}] \right\}$.

where $i \in \{1, 2\}$.

Group	Structure
$P \rtimes \left\langle T, A^{q^{e_0 - c_0}}, B^{s/d} \right\rangle$	$(N \rtimes (C_p \rtimes C_{q^{c_0}})) \rtimes C_d$
$P \rtimes \left\langle TA^{uq^{e_0 - c_0}}, B^{s/d} \right\rangle, (c_0, u) \neq (0, u), (1, -1)$	$\mathbb{F}_p^2 \rtimes_u C_{dq^{c_0}}$
$P \rtimes \left\langle T, B^{s/d} \right\rangle$	$((C_p \rtimes C_q) \times C_p) \rtimes C_d$
$\langle \mathbf{e}_1, T, B^{s/d} \rangle$	$C_p \rtimes C_{dq}$
$\langle \mathbf{e}_1, TA^{uq^{e_0 - c_0}}, B^{s/d} \rangle, (c_0, u) \neq (0, u), (1, -1)$	$C_p \rtimes C_{dq^{c_0}}$
$\langle \mathbf{e}_1, TA^{-q^{e_0 - 1}}, B^{s/d} \rangle$	$(C_p \rtimes C_d) \times C_q$
$\langle \mathbf{e}_1, T, A^{q^{e_0 - c_0}}, B^{s/d} \rangle$	$(C_p \rtimes C_{dq^{c_0}}) \times C_q$
$\langle \mathbf{e}_2, TA^{-q^{e_0 - 1}}, B^{s/d} \rangle$	$C_p \rtimes C_{dq}$
$\langle \mathbf{e}_2, T, B^{s/d} \rangle$	$(C_p \rtimes C_d) \times C_q$

Table: Isomorphism types of transitive groups for N metabelian.

Group	Structure
$\langle \mathbf{e}_2, TA^{uq^{e_0-c_0}}, B^{s/d} \rangle$	$C_p \rtimes C_{dq^{c_0}}$
$\langle \mathbf{e}_2, T, A^{q^{e_0-c_0}}, B^{s/d} \rangle$	$(C_p \rtimes C_{dq^{c_0}}) \times C_q$
$\langle \mathbf{e}_1, T \rangle$	$C_p \rtimes C_q$
$\langle \mathbf{e}_1, TA^{uq^{e_0-c_0}} \rangle$, $(c_0, u) \neq (0, u), (1, -1)$	$C_p \rtimes C_{q^{c_0}}$
$\langle \mathbf{e}_1, TA^{-q^{e_0-1}} \rangle$	C_{pq}
$\langle \mathbf{e}_1, T, A^{q^{e_0-c_0}} \rangle$	$(C_p \rtimes C_{q^{c_0}}) \times C_q$
$\langle \mathbf{e}_2, TA^{-q^{e_0-1}} \rangle$	$C_p \rtimes C_q$
$\langle \mathbf{e}_2, T \rangle$	C_{pq}
$\langle \mathbf{e}_2, TA^{uq^{e_0-c_0}} \rangle$	$C_p \rtimes C_{q^{c_0}}$
$\langle \mathbf{e}_2, T, A^{q^{e_0-c_0}} \rangle$	$(C_p \rtimes C_{q^{c_0}}) \times C_q$

Table: Isomorphism types of transitive groups for N metabelian.

$M' = M \cap \mathrm{Aut}(N) = M \cap \langle \mathbf{e}_1 - \mathbf{e}_2, A, B \rangle$

Structure	#groups	$\lvert\mathrm{Aut}(M, M')\rvert$	#HGS
$(N \rtimes (C_p \rtimes C_{q^{c_0}})) \rtimes C_d,\ c_0 \neq 0$	1	$2p(p-1)$	2
$(C_p \rtimes C_q) \times C_p$ $\mathbb{F}_p^2 \rtimes_u C_{q^{c_0}},\ (c_0, u) \neq (0, u), (1, -1),$ $u \in (\mathbb{Z}/q^{c_0}\mathbb{Z})^\times \setminus \{\frac{1}{2}(q^{c_0} - q^{c_0-1})\}$ $\mathbb{F}_p^2 \rtimes_{\frac{1}{2}(q^{c_0}-q^{c_0-1})} C_{q^{c_0}},\ c_0 \neq 0$	2 2 1	$p^2(p-1)$ $p^2(p-1)$ $2p^2(p-1)$	$2p$ $2p$ $2p$
$(C_p \times (C_p \rtimes C_q)) \rtimes C_d,\ d > 1$ $\mathbb{F}_p^2 \rtimes_u C_{dq^{c_0}},\ (c_0, u) \neq (0, u), (1, -1), d > 1$ $u \in (\mathbb{Z}/q^{c_0}\mathbb{Z})^\times \setminus \{\frac{1}{2}(q^{c_0} - q^{c_0-1})\}$ $\mathbb{F}_p^2 \rtimes_{\frac{1}{2}(q^{c_0}-q^{c_0-1})} C_{dq^{c_0}},\ c_0 \neq 0, d > 1$	2 2 1	$p(p-1)$ $p(p-1)$ $2p(p-1)$	2 2 2
$C_p \rtimes C_{dq^{c_0}},\ (c_0, d) \neq (1, 1), (0, d)$	$2p\varphi(q^{c_0})$	$p-1$	$2\varphi(q^{c_0})$
$C_p \rtimes C_q$	$2p(q-1)+2$	$p(p-1)$	$2p(q-2)+2$
$(C_p \rtimes C_{dq^{c_0}}) \times C_q$	$2p$	$(p-1)(q-1)$	$2(q-1)$

Table: Transitive subgroups for N metabelian.

Theorem 2.6

In total, there are

$$\sigma_0(s)\left[3e_0 + 2 + \frac{1}{2}(q^{e_0} - 1)\right]$$

isomorphism types of permutation groups G of degree pq which are realised by Hopf-Galois structures of non-abelian type $C_p \rtimes C_q$.

Structure	# cyclic type HGS	# non-abelian type HGS
$(C_p \rtimes C_{dq^{c_0}}) \times C_q$	1	$2(q-1)$
$C_p \rtimes C_{dq^{c_0}}$, $(c_0, d) \neq (1,1), (0,d)$	1	$2\varphi(q^{c_0})$
$C_p \rtimes C_q$	p	$2p(q-2)+2$

Table: Groups admitting Hopf-Galois structures of both types.

Remark 2.7

Specialising to the Sophie Germain case, we obtain $2(3+2+\frac{1}{2}(q-1)) = q+9$ *isomorphism types. This retrieves the result of Byott & Martin-Lyons.*

Remark 2.7

Specialising to the Sophie Germain case, we obtain $2(3+2+\frac{1}{2}(q-1)) = q+9$ *isomorphism types. This retrieves the result of Byott & Martin-Lyons.*

Main comparisons:

- The arbitrary e_0 introduces *many* more groups to work with.

Remark 2.7

Specialising to the Sophie Germain case, we obtain $2(3+2+\frac{1}{2}(q-1)) = q+9$ *isomorphism types. This retrieves the result of Byott & Martin-Lyons.*

Main comparisons:

- The arbitrary e_0 introduces *many* more groups to work with.
- We think about $u \in (\mathbb{Z}/q^{c_0}\mathbb{Z})^{\times}$ instead of just $1 \leq u \leq q-1$.

Remark 2.7

Specialising to the Sophie Germain case, we obtain $2(3+2+\frac{1}{2}(q-1)) = q+9$ *isomorphism types. This retrieves the result of Byott & Martin-Lyons.*

Main comparisons:

- The arbitrary e_0 introduces *many* more groups to work with.
- We think about $u \in (\mathbb{Z}/q^{c_0}\mathbb{Z})^\times$ instead of just $1 \leq u \leq q-1$.
- groups of the same order seem to reflect Sophie-Germain case - there aren't many more starkly different structures arising.

Remark 2.7

Specialising to the Sophie Germain case, we obtain $2(3 + 2 + \frac{1}{2}(q-1)) = q + 9$ *isomorphism types. This retrieves the result of Byott & Martin-Lyons.*

Main comparisons:

- The arbitrary e_0 introduces *many* more groups to work with.
- We think about $u \in (\mathbb{Z}/q^{c_0}\mathbb{Z})^\times$ instead of just $1 \leq u \leq q-1$.
- groups of the same order seem to reflect Sophie-Germain case - there aren't many more starkly different structures arising.
- $B^{s/d}$ behaves almost exactly the same as to when $s = 2$ in Sophie-Germain.

Intermediate fields

L/K is only one degree pq intermediate field between E and K. What about the others? There's no guarantee that the Hopf-Galois structures on these fields F even exist!

Intermediate fields

L/K is only one degree pq intermediate field between E and K. What about the others? There's no guarantee that the Hopf-Galois structures on these fields F even exist!

Recall the two groups G and G'; together we can consider the pair (G, G') a permutation group. Here G' is a subgroup of index n and trivial *core*, that is

$$\mathrm{Core}_G(G') = \cap_{g \in G} g G' g^{-1} = \{1\}\,.$$

We work with the index pq subgroups H of G (so that $F = H^E$).

Intermediate fields

The possibilities:

Intermediate fields

The possibilities:

- H is conjugate to G' (thus F is conjugate to L).

Intermediate fields

The possibilities:

- H is conjugate to G' (thus F is conjugate to L).
- H is not conjugate to G', but there is some $\phi \in \mathrm{Aut}(G)$ with $\phi(G') = H$.

Intermediate fields

The possibilities:

- H is conjugate to G' (thus F is conjugate to L).
- H is not conjugate to G', but there is some $\phi \in \mathrm{Aut}(G)$ with $\phi(G') = H$.
- G' and H lie in separate $\mathrm{Aut}(G)$-orbits, but $\mathrm{Core}_G(H) := \bigcap_{g \in G} gHg^{-1} = \{1\}$.

Intermediate fields

The possibilities:

- H is conjugate to G' (thus F is conjugate to L).
- H is not conjugate to G', but there is some $\phi \in \mathrm{Aut}(G)$ with $\phi(G') = H$.
- G' and H lie in separate $\mathrm{Aut}(G)$-orbits, but $\mathrm{Core}_G(H) := \bigcap_{g \in G} gHg^{-1} = \{1\}$.
  - H and G' may or may not be isomorphic as abstract groups.

Intermediate fields

The possibilities:

- H is conjugate to G' (thus F is conjugate to L).
- H is not conjugate to G', but there is some $\phi \in \mathrm{Aut}(G)$ with $\phi(G') = H$.
- G' and H lie in separate $\mathrm{Aut}(G)$-orbits, but $\mathrm{Core}_G(H) := \bigcap_{g \in G} gHg^{-1} = \{1\}$.
  - H and G' may or may not be isomorphic as abstract groups.
  - F/K may or may not admit a Hopf-Galois structure; if it does, then (G, H) will show up as a transitive subgroup of $\mathrm{Hol}(N)$ for some N of order n.

Intermediate fields

The possibilities:

- H is conjugate to G' (thus F is conjugate to L).
- H is not conjugate to G', but there is some $\phi \in \text{Aut}(G)$ with $\phi(G') = H$.
- G' and H lie in separate $\text{Aut}(G)$-orbits, but $\text{Core}_G(H) := \bigcap_{g \in G} gHg^{-1} = \{1\}$.
  - H and G' may or may not be isomorphic as abstract groups.
  - F/K may or may not admit a Hopf-Galois structure; if it does, then (G, H) will show up as a transitive subgroup of $\text{Hol}(N)$ for some N of order n.
- G' and H lie in separate $\text{Aut}(G)$-orbits and $C := \text{Core}_G(H) \neq \{1\}$, and so F would have smaller normal closure, E^C, yielding the permutation group $(G/C, H/C)$.

Intermediate fields

The possibilities:

- H is conjugate to G' (thus F is conjugate to L).
- H is not conjugate to G', but there is some $\phi \in \mathrm{Aut}(G)$ with $\phi(G') = H$.
- G' and H lie in separate $\mathrm{Aut}(G)$-orbits, but $\mathrm{Core}_G(H) := \bigcap_{g \in G} gHg^{-1} = \{1\}$.
  - H and G' may or may not be isomorphic as abstract groups.
  - F/K may or may not admit a Hopf-Galois structure; if it does, then (G, H) will show up as a transitive subgroup of $\mathrm{Hol}(N)$ for some N of order n.
- G' and H lie in separate $\mathrm{Aut}(G)$-orbits and $C := \mathrm{Core}_G(H) \neq \{1\}$, and so F would have smaller normal closure, E^C, yielding the permutation group $(G/C, H/C)$.
  - We again ask ourselves if this corresponds to a transitive subgroup of some $\mathrm{Hol}(N)$.

Intermediate fields

We compute the index pq subgroups H of G and categorise them in terms of

Intermediate fields

We compute the index pq subgroups H of G and categorise them in terms of

- conjugacy class,

Intermediate fields

We compute the index pq subgroups H of G and categorise them in terms of

- conjugacy class,
- orbits under $\mathrm{Aut}(G)$,

Intermediate fields

We compute the index pq subgroups H of G and categorise them in terms of

- conjugacy class,
- orbits under $\mathrm{Aut}(G)$,
- abstract isomorphism class.

Intermediate fields

We compute the index pq subgroups H of G and categorise them in terms of

- conjugacy class,
- orbits under $\mathrm{Aut}(G)$,
- abstract isomorphism class.

We also need to compute $C = \mathrm{Core}_G(H)$, and then we take G/C to see if it appears in the list of transitive subgroups of $\mathrm{Hol}(N)$. **For $\mathbf{n = pq}$, we find that all intermediate field extensions admit at least one Hopf-Galois structure.**

Intermediate fields

For $p = 2q + 1$, it is feasible to compute everything very explicitly. However, making use of a generalisation of Sylow's theorems, we can approach the problem very efficiently even for the general pq case. In short, the work can be summarised in the following two tables:

Subgroup condition	#Conj. classes	#Aut(G)-orbits	#Isom. classes
$q^2 \nmid \lvert G \rvert$	1	1	1
$q^2 \mid \lvert G \rvert$, not (*)	2	2	2
$q^2 \mid \lvert G \rvert$, (*)	2	2	1

Table: Results for index pq subgroups of $Hol(N)$ for N cyclic.

Where (*) is the condition that G contains no automorphisms with order coprime to pq, along with $c_0 = 1$.

Intermediate fields

For $p = 2q + 1$, it is feasible to compute everything very explicitly. However, making use of a generalisation of Sylow's theorems, we can approach the problem very efficiently even for the general pq case. In short, the work can be summarised in the following two tables:

Order of index pq subgroup	#Conj. classes
pd	4
$pq^{c_0-1}d$, $c_0 > 1$	$4(q+1)$
$pq^{c_0}d$, $c_0 > 0$	$4(q+1)$
d	1
$q^{c_0-1}d$, $c_0 > 1$	$q+1$
$q^{c_0}d$, $c_0 > 0$	$q+1$

Table: Results for index pq subgroups of $Hol(N)$ for N metabelian.

Intermediate fields

For $p = 2q + 1$, it is feasible to compute everything very explicitly. However, making use of a generalisation of Sylow's theorems, we can approach the problem very efficiently even for the general pq case. In short, the work can be summarised in the following two tables:

#Aut(G)-orbits	#Isom. classes
2 if $(c_0, u) = (1, \frac{1}{2}(q-1))$, 3 otherwise	1
3	1
$q + 3$ if $c_0 = 1$, $\varphi(q^{c_0}) + 6$ otherwise	2
1	1
1	1
2	2

Table: Results for index pq subgroups of $Hol(N)$ for N metabelian.

Intermediate fields

There is a pattern in the tables; it looks like the groups divisible by the same powers of p and q behave pretty much the same regardless of the other factors coprime to pq.

Intermediate fields

There is a pattern in the tables; it looks like the groups divisible by the same powers of p and q behave pretty much the same regardless of the other factors coprime to pq.

- Hall's theorem tells us why this is the case for conjugacy classes.

Intermediate fields

There is a pattern in the tables; it looks like the groups divisible by the same powers of p and q behave pretty much the same regardless of the other factors coprime to pq.

- Hall's theorem tells us why this is the case for conjugacy classes.
- It can be proved that this is the case for the $\mathrm{Aut}(G)$ orbits for the general pq case, but for more general squarefree n, the arguments look like they are a little more subtle.

Intermediate fields

There is a pattern in the tables; it looks like the groups divisible by the same powers of p and q behave pretty much the same regardless of the other factors coprime to pq.

- Hall's theorem tells us why this is the case for conjugacy classes.
- It can be proved that this is the case for the $\mathrm{Aut}(G)$ orbits for the general pq case, but for more general squarefree n, the arguments look like they are a little more subtle.

It may also be the case that for more general squarefree n, we find intermediate fields which *don't* admit Hopf-Galois structures...

What's next?

There are a few ways to generalise:

What's next?

There are a few ways to generalise:

- pqr, p, q, r distinct odd primes,

What's next?

There are a few ways to generalise:

- pqr, p, q, r distinct odd primes,
- $p = 2q + 1, q = 2r + 1$, $(p, q), (q, r)$ safe prime - Sophie Germain prime pair,

What's next?

There are a few ways to generalise:

- pqr, p, q, r distinct odd primes,
- $p = 2q + 1, q = 2r + 1$, $(p, q), (q, r)$ safe prime - Sophie Germain prime pair,
- $p_1 = 2p_2 + 1, p_2 = 2p_3 + 1, \cdots, p_{m-1} = 2p_m + 1$, Cunningham chain of length m,

What's next?

There are a few ways to generalise:

- pqr, p, q, r distinct odd primes,
- $p = 2q + 1, q = 2r + 1$, $(p, q), (q, r)$ safe prime - Sophie Germain prime pair,
- $p_1 = 2p_2 + 1, p_2 = 2p_3 + 1, \cdots, p_{m-1} = 2p_m + 1$, Cunningham chain of length m,
- general squarefree separable extensions.

pqr

Let $n = pqr$ where $p > q > r$ distinct odd primes.

pqr

Let $n = pqr$ where $p > q > r$ distinct odd primes.

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

where $pqr = de$, $\mathrm{ord}_e(k) = d$. Further, let $z = \gcd(k-1, e)$, and $g = e/z$. Due to the conditions in [Byo96], we obtain the following six factorisations, giving rise to $r+4$ groups:

d	g	z	Condition	#groups
1	1	pqr		1
r	q	p	$q \equiv 1 \pmod{r}$	1
r	p	q	$p \equiv 1 \pmod{r}$	1
r	qp	1	$q \equiv p \equiv 1 \pmod{r}$	$r-1$
q	p	r	$p \equiv 1 \pmod{q}$	1
rq	p	1	$p \equiv 1 \pmod{rq}$	1

Table: Groups of order *pqr*

Let $N = C_{pqr} = \langle \sigma, \tau, \rho \mid \sigma^p = \tau^q = \rho^r = 1, \text{abelian} \rangle$, with

$$p - 1 = r^{e_r} q^{e_q} \ell_1^{e_1} \cdots \ell_s^{e_m},$$
$$q - 1 = q^{f_q} \ell_1^{f_1} \cdots \ell_s^{f_m},$$
$$r - 1 = \ell_1^{h_1} \cdots \ell_s^{h_m}.$$

Let $N = C_{pqr} = \langle \sigma, \tau, \rho \mid \sigma^p = \tau^q = \rho^r = 1, \text{abelian} \rangle$, with

$$p - 1 = r^{e_r} q^{e_q} \ell_1^{e_1} \cdots \ell_s^{e_m},$$
$$q - 1 = q^{f_q} \ell_1^{f_1} \cdots \ell_s^{f_m},$$
$$r - 1 = \ell_1^{h_1} \cdots \ell_s^{h_m}.$$

Let

$$\alpha \in \text{Aut}(\langle \sigma \rangle) \text{ of order } r^{e_r},$$
$$\beta \in \text{Aut}(\langle \sigma \rangle) \text{ of order } q^{e_q},$$
$$\alpha_i \in \text{Aut}(\langle \sigma \rangle) \text{ of order } \ell_i^{e_i},$$
$$\gamma \in \text{Aut}(\langle \tau \rangle) \text{ of order } r^{f_r},$$
$$\beta_i \in \text{Aut}(\langle \tau \rangle) \text{ of order } \ell_i^{f_i},$$
$$\gamma_i \in \text{Aut}(\langle \rho \rangle) \text{ of order } \ell_i^{h_i}.$$

Let $N = C_{pqr} = \langle \sigma, \tau, \rho \mid \sigma^p = \tau^q = \rho^r = 1, \text{abelian} \rangle$, with

$$\begin{aligned} p - 1 &= r^{e_r} q^{e_q} \ell_1^{e_1} \cdots \ell_s^{e_m}, \\ q - 1 &= q^{f_q} \ell_1^{f_1} \cdots \ell_s^{f_m}, \\ r - 1 &= \ell_1^{h_1} \cdots \ell_s^{h_m}. \end{aligned}$$

Let

$$\begin{aligned} &\alpha \in \text{Aut}(\langle \sigma \rangle) \text{ of order } r^{e_r}, \\ &\beta \in \text{Aut}(\langle \sigma \rangle) \text{ of order } q^{e_q}, \\ &\alpha_i \in \text{Aut}(\langle \sigma \rangle) \text{ of order } \ell_i^{e_i}, \\ &\gamma \in \text{Aut}(\langle \tau \rangle) \text{ of order } r^{f_r}, \\ &\beta_i \in \text{Aut}(\langle \tau \rangle) \text{ of order } \ell_i^{f_i}, \\ &\gamma_i \in \text{Aut}(\langle \rho \rangle) \text{ of order } \ell_i^{h_i}. \end{aligned}$$

So

$$\text{Aut}(N) \cong \langle \beta \rangle \times \langle \alpha, \gamma \rangle \times \langle \alpha_1, \beta_1, \gamma_1 \rangle \times \cdots \times \langle \alpha_m, \beta_m, \gamma_m \rangle.$$

The following are the transitive subgroups of the unique Hall $\{p, q, r\}$-subgroup $H = \langle \sigma, \tau, \rho, \alpha, \beta, \gamma \rangle$:

(A) $N \cong C_{pqr}$,

(B) $\langle \sigma, \rho, [\tau, \beta^{tq^{e_q - d}}] \rangle \cong (C_p \rtimes C_{q^d}) \times C_r$,

(C) $\langle \sigma, \tau, [\rho^{x_1}, \alpha^{t_1 r^{e_r - e}} \gamma^{s_1 r^{f_r - f}}] \rangle \cong C_{pq} \rtimes C_r$,

(D) $\langle \sigma, [\tau, \beta^{tq^{e_q - d}}], [\rho, \alpha^{sr^{f_r - f}}] \rangle \cong C_p \rtimes C_{q^d r^f}$

The following are the transitive subgroups of the unique Hall $\{p, q, r\}$-subgroup $H = \langle \sigma, \tau, \rho, \alpha, \beta, \gamma \rangle$:

$$
\begin{aligned}
&\text{(A) } N \cong C_{pqr}, \\
&\text{(B) } \langle \sigma, \rho, [\tau, \beta^{tq^{e_q - d}}] \rangle \cong (C_p \rtimes C_{q^d}) \times C_r, \\
&\text{(C) } \langle \sigma, \tau, [\rho^{x_1}, \alpha^{t_1 r^{e_r - e}} \gamma^{s_1 r^{f_r - f}}] \rangle \cong C_{pq} \rtimes C_r, \\
&\text{(D) } \langle \sigma, [\tau, \beta^{tq^{e_q - d}}], [\rho, \alpha^{sr^{f_r - f}}] \rangle \cong C_p \rtimes C_{q^d r^f}
\end{aligned}
$$

We see that (A) is normalised by $\mathrm{Aut}(N)$, (B) is normalised by $\mathrm{Aut}(\langle \sigma \rangle) \times \mathrm{Aut}(\langle \rho \rangle)$, (C) is normalised by $\mathrm{Aut}(\langle \sigma \rangle) \times \mathrm{Aut}(\langle \tau \rangle)$, and (D) is normalised by $\mathrm{Aut}(\langle \sigma \rangle)$

We now have the problem of finding subgroups of $\langle \alpha_i, \beta_i, \gamma_i \rangle$.

We now have the problem of finding subgroups of $\langle \alpha_i, \beta_i, \gamma_i \rangle$. We now ask "what are the subgroups of an arbitrary abelian rank 3 ℓ_i-group?";

We now have the problem of finding subgroups of $\langle \alpha_i, \beta_i, \gamma_i \rangle$. We now ask "what are the subgroups of an arbitrary abelian rank 3 ℓ_i-group?"; in more generality (for $n = p_1 \cdots p_m$), we have the problem of finding all subgroups of an arbitrary rank m ℓ_i-group. **This is a hard problem in general**.

We now have the problem of finding subgroups of $\langle \alpha_i, \beta_i, \gamma_i \rangle$. We now ask "what are the subgroups of an arbitrary abelian rank 3 ℓ_i-group?"; in more generality (for $n = p_1 \cdots p_m$), we have the problem of finding all subgroups of an arbitrary rank m ℓ_i-group. **This is a hard problem in general**.
Ideas

- There is a concrete formula known for $m = 3$.

We now have the problem of finding subgroups of $\langle \alpha_i, \beta_i, \gamma_i \rangle$. We now ask "what are the subgroups of an arbitrary abelian rank 3 ℓ_i-group?"; in more generality (for $n = p_1 \cdots p_m$), we have the problem of finding all subgroups of an arbitrary rank m ℓ_i-group. **This is a hard problem in general**.
Ideas

- There is a concrete formula known for $m = 3$.
- No concrete formula exists for $m > 3$, but there are algorithms and asymptotic formulae.

We now have the problem of finding subgroups of $\langle \alpha_i, \beta_i, \gamma_i \rangle$. We now ask "what are the subgroups of an arbitrary abelian rank 3 ℓ_i-group?"; in more generality (for $n = p_1 \cdots p_m$), we have the problem of finding all subgroups of an arbitrary rank m ℓ_i-group. **This is a hard problem in general**.

Ideas

- There is a concrete formula known for $m = 3$.
- No concrete formula exists for $m > 3$, but there are algorithms and asymptotic formulae.
- We can focus on the general forms of these subgroups, which we can obtain by looking at row echelon forms of $m \times m$ matrices.

We now have the problem of finding subgroups of $\langle \alpha_i, \beta_i, \gamma_i \rangle$. We now ask "what are the subgroups of an arbitrary abelian rank 3 ℓ_i-group?"; in more generality (for $n = p_1 \cdots p_m$), we have the problem of finding all subgroups of an arbitrary rank m ℓ_i-group. **This is a hard problem in general**.

Ideas

- There is a concrete formula known for $m = 3$.
- No concrete formula exists for $m > 3$, but there are algorithms and asymptotic formulae.
- We can focus on the general forms of these subgroups, which we can obtain by looking at row echelon forms of $m \times m$ matrices.
- For $m = 3$, there are seven distinct forms.

We now have the problem of finding subgroups of $\langle \alpha_i, \beta_i, \gamma_i \rangle$. We now ask "what are the subgroups of an arbitrary abelian rank 3 ℓ_i-group?"; in more generality (for $n = p_1 \cdots p_m$), we have the problem of finding all subgroups of an arbitrary rank m ℓ_i-group. **This is a hard problem in general**.
Ideas

- There is a concrete formula known for $m = 3$.
- No concrete formula exists for $m > 3$, but there are algorithms and asymptotic formulae.
- We can focus on the general forms of these subgroups, which we can obtain by looking at row echelon forms of $m \times m$ matrices.
- For $m = 3$, there are seven distinct forms.
- In general, there are $2^m - 1$ possible row echelon forms (or 2^m including the zero matrix).

We now have the problem of finding subgroups of $\langle \alpha_i, \beta_i, \gamma_i \rangle$. We now ask "what are the subgroups of an arbitrary abelian rank 3 ℓ_i-group?"; in more generality (for $n = p_1 \cdots p_m$), we have the problem of finding all subgroups of an arbitrary rank m ℓ_i-group. **This is a hard problem in general**.

Ideas

- There is a concrete formula known for $m = 3$.
- No concrete formula exists for $m > 3$, but there are algorithms and asymptotic formulae.
- We can focus on the general forms of these subgroups, which we can obtain by looking at row echelon forms of $m \times m$ matrices.
- For $m = 3$, there are seven distinct forms.
- In general, there are $2^m - 1$ possible row echelon forms (or 2^m including the zero matrix).
- Restrict the relationship between the primes in the factorisation of n.

Cunningham chains

Let $n = p_1 \cdots p_m$, where $p_1 = 2p_2 + 1, \cdots, p_{m-1} = 2p_m + 1$ (they form a Cunningham chain of length m).

Cunningham chains

Let $n = p_1 \cdots p_m$, where $p_1 = 2p_2 + 1, \cdots, p_{m-1} = 2p_m + 1$ (they form a Cunningham chain of length m).

Conjecture 3.1

For any natural number m, there are infinitely many Cunningham chains of length m.

Cunningham chains

Let $n = p_1 \cdots p_m$, where $p_1 = 2p_2 + 1, \cdots, p_{m-1} = 2p_m + 1$ (they form a Cunningham chain of length m).

Conjecture 3.1

For any natural number m, there are infinitely many Cunningham chains of length m.

There are m different abstract groups of order n:

Cunningham chains

Let $n = p_1 \cdots p_m$, where $p_1 = 2p_2 + 1, \cdots, p_{m-1} = 2p_m + 1$ (they form a Cunningham chain of length m).

Conjecture 3.1

For any natural number m, there are infinitely many Cunningham chains of length m.

There are m different abstract groups of order n:

- $N \cong C_n$,

Cunningham chains

Let $n = p_1 \cdots p_m$, where $p_1 = 2p_2 + 1, \cdots, p_{m-1} = 2p_m + 1$ (they form a Cunningham chain of length m).

Conjecture 3.1

For any natural number m, there are infinitely many Cunningham chains of length m.

There are m different abstract groups of order n:

- $N \cong C_n$,
- $N_i \cong C_{p_1} \times C_{p_2} \times \cdots \times (C_{p_i} \rtimes C_{p_{i+1}}) \times \cdots \times C_{p_{m-1}} \times C_{p_l}, 1 \leq i \leq m-1$.

Cunningham chains

Let $n = p_1 \cdots p_m$, where $p_1 = 2p_2 + 1, \cdots, p_{m-1} = 2p_m + 1$ (they form a Cunningham chain of length m).

Conjecture 3.1

For any natural number m, there are infinitely many Cunningham chains of length m.

There are m different abstract groups of order n:

- $N \cong C_n$,
- $N_i \cong C_{p_1} \times C_{p_2} \times \cdots \times (C_{p_i} \rtimes C_{p_{i+1}}) \times \cdots \times C_{p_{m-1}} \times C_{p_l}, 1 \leq i \leq m-1$.

Remark 3.2

The special case $m = 2$ (where $p = 2q + 1$ with (p, q) a safe prime - Sophie Germain prime pair) is given by the work of Byott and Martin-Lyons in [BML22].

Cunningham chains

Let $n = p_1 \cdots p_m$, where $p_1 = 2p_2 + 1, \cdots, p_{m-1} = 2p_m + 1$ (they form a Cunningham chain of length m).

Conjecture 3.1

For any natural number m, there are infinitely many Cunningham chains of length m.

There are m different abstract groups of order n:

- $N \cong C_n$,
- $N_i \cong C_{p_1} \times C_{p_2} \times \cdots \times (C_{p_i} \rtimes C_{p_{i+1}}) \times \cdots \times C_{p_{m-1}} \times C_{p_l}, 1 \leq i \leq m-1.$

Remark 3.2

The special case $m = 2$ (where $p = 2q + 1$ with (p, q) a safe prime - Sophie Germain prime pair) is given by the work of Byott and Martin-Lyons in [BML22].

We can treat all the N_i in one discussion. Thus we have the two cases of $\mathrm{Hol}(C_n)$, and $\mathrm{Hol}(N_i) \cong \mathrm{Hol}(C_{n/p_i p_{i+1}}) \times \mathrm{Hol}(C_{p_i} \rtimes C_{p_{i+1}})$.

For $N \cong C_n$, we have $\mathrm{Aut}(N)$ is generated by:

$\alpha_1, \beta_1 \in \mathrm{Aut}(\langle\sigma_1\rangle)$ of orders $p_2, 2$ respectively,

$\alpha_2, \beta_2 \in \mathrm{Aut}(\langle\sigma_2\rangle)$ of orders $p_3, 2$ respectively,

$\vdots$

$\alpha_{m-1}, \beta_{m-1} \in \mathrm{Aut}(\langle\sigma_{m-1}\rangle)$ of orders $p_m, 2$ respectively,

$\gamma, \delta \in \mathrm{Aut}(\langle\sigma_m\rangle)$ of orders $2^x, s$ respectively.

For $N \cong C_n$, we have $\mathrm{Aut}(N)$ is generated by:

$$\begin{aligned}
&\alpha_1, \beta_1 \in \mathrm{Aut}(\langle \sigma_1 \rangle) \text{ of orders } p_2, 2 \text{ respectively,}\\
&\alpha_2, \beta_2 \in \mathrm{Aut}(\langle \sigma_2 \rangle) \text{ of orders } p_3, 2 \text{ respectively,}\\
&\vdots\\
&\alpha_{m-1}, \beta_{m-1} \in \mathrm{Aut}(\langle \sigma_{m-1} \rangle) \text{ of orders } p_m, 2 \text{ respectively,}\\
&\gamma, \delta \in \mathrm{Aut}(\langle \sigma_m \rangle) \text{ of orders } 2^x, s \text{ respectively.}
\end{aligned}$$

Thus

$$\mathrm{Hol}(N) = \langle \sigma_1, \cdots, \sigma_m \rangle \rtimes (\langle \alpha_1 \rangle \times \cdots \times \langle \alpha_{m-1} \rangle \times \langle \beta_1, \cdots, \beta_{m-1}, \gamma \rangle \times \langle \delta \rangle)$$

For $N \cong C_n$, we have Aut(N) is generated by:

$$\begin{aligned}
&\alpha_1, \beta_1 \in \text{Aut}(\langle \sigma_1 \rangle) \text{ of orders } p_2, 2 \text{ respectively,}\\
&\alpha_2, \beta_2 \in \text{Aut}(\langle \sigma_2 \rangle) \text{ of orders } p_3, 2 \text{ respectively,}\\
&\vdots\\
&\alpha_{m-1}, \beta_{m-1} \in \text{Aut}(\langle \sigma_{m-1} \rangle) \text{ of orders } p_m, 2 \text{ respectively,}\\
&\gamma, \delta \in \text{Aut}(\langle \sigma_m \rangle) \text{ of orders } 2^x, s \text{ respectively.}
\end{aligned}$$

Thus

$$\text{Hol}(N) = \langle \sigma_1, \cdots, \sigma_m \rangle \rtimes (\langle \alpha_1 \rangle \times \cdots \times \langle \alpha_{m-1} \rangle \times \langle \beta_1, \cdots, \beta_{m-1}, \gamma \rangle \times \langle \delta \rangle)$$

We will need to find the subgroups of Aut(N), and in particular, the subgroups of the rank l abelian 2-group $\langle \beta_1, \cdots, \beta_{m-1}, \gamma \rangle$.

For $N \cong C_n$, we have $\mathrm{Aut}(N)$ is generated by:

$$\alpha_1, \beta_1 \in \mathrm{Aut}(\langle \sigma_1 \rangle) \text{ of orders } p_2, 2 \text{ respectively,}$$
$$\alpha_2, \beta_2 \in \mathrm{Aut}(\langle \sigma_2 \rangle) \text{ of orders } p_3, 2 \text{ respectively,}$$
$$\vdots$$
$$\alpha_{m-1}, \beta_{m-1} \in \mathrm{Aut}(\langle \sigma_{m-1} \rangle) \text{ of orders } p_m, 2 \text{ respectively,}$$
$$\gamma, \delta \in \mathrm{Aut}(\langle \sigma_m \rangle) \text{ of orders } 2^x, s \text{ respectively.}$$

Thus

$$\mathrm{Hol}(N) = \langle \sigma_1, \cdots, \sigma_m \rangle \rtimes (\langle \alpha_1 \rangle \times \cdots \times \langle \alpha_{m-1} \rangle \times \langle \beta_1, \cdots, \beta_{m-1}, \gamma \rangle \times \langle \delta \rangle)$$

We will need to find the subgroups of $\mathrm{Aut}(N)$, and in particular, the subgroups of the rank l abelian 2-group $\langle \beta_1, \cdots, \beta_{m-1}, \gamma \rangle$. For this, we use a known result of the number of subgroups of $(C_2)^l$, and modify:

For $N \cong C_n$, we have $\mathrm{Aut}(N)$ is generated by:

$$\begin{aligned}
&\alpha_1, \beta_1 \in \mathrm{Aut}(\langle \sigma_1 \rangle) \text{ of orders } p_2, 2 \text{ respectively},\\
&\alpha_2, \beta_2 \in \mathrm{Aut}(\langle \sigma_2 \rangle) \text{ of orders } p_3, 2 \text{ respectively},\\
&\vdots\\
&\alpha_{m-1}, \beta_{m-1} \in \mathrm{Aut}(\langle \sigma_{m-1} \rangle) \text{ of orders } p_m, 2 \text{ respectively},\\
&\gamma, \delta \in \mathrm{Aut}(\langle \sigma_m \rangle) \text{ of orders } 2^x, s \text{ respectively}.
\end{aligned}$$

Thus

$$\mathrm{Hol}(N) = \langle \sigma_1, \cdots, \sigma_m \rangle \rtimes (\langle \alpha_1 \rangle \times \cdots \times \langle \alpha_{m-1} \rangle \times \langle \beta_1, \cdots, \beta_{m-1}, \gamma \rangle \times \langle \delta \rangle)$$

We will need to find the subgroups of $\mathrm{Aut}(N)$, and in particular, the subgroups of the rank l abelian 2-group $\langle \beta_1, \cdots, \beta_{m-1}, \gamma \rangle$. For this, we use a known result of the number of subgroups of $(C_2)^l$, and modify:

$$\Sigma_m := x \sum_{k=0}^{l} \prod_{i=1}^{l-k} \frac{2^{i+k}-1}{2^i-1} + (1-x) \sum_{k=0}^{m-1} \prod_{i=1}^{m-1-k} \frac{2^{i+k}-1}{2^i-1}.$$

The regular subgroups of $\mathrm{Hol}(N)$ are of the form

$$\langle \sigma_1, [\sigma_2, \alpha_1^{t_1}], \cdots, [\sigma_l, \alpha_{m-1}^{t_{m-1}}] \rangle$$

where all but possibly one t_i are zero, and in the case that $t_j \neq 0$, we have $1 \leq t_j \leq p_{j+1} - 1$.

The regular subgroups of $\mathrm{Hol}(N)$ are of the form

$$\langle \sigma_1, [\sigma_2, \alpha_1^{t_1}], \cdots, [\sigma_l, \alpha_{m-1}^{t_{m-1}}] \rangle$$

where all but possibly one t_i are zero, and in the case that $t_j \neq 0$, we have $1 \leq t_j \leq p_{j+1} - 1$.All transitive subgroups of $\mathrm{Hol}(N)$ are given by $J \rtimes A$, where J is a regular subgroup of $\mathrm{Hol}(N)$ and A is some subgroup of $\mathrm{Aut}(N)$ which normalises J.

The regular subgroups of $\mathrm{Hol}(N)$ are of the form

$$\langle \sigma_1, [\sigma_2, \alpha_1^{t_1}], \cdots, [\sigma_l, \alpha_{m-1}^{t_{m-1}}] \rangle$$

where all but possibly one t_i are zero, and in the case that $t_j \neq 0$, we have $1 \leq t_j \leq p_{j+1} - 1$.All transitive subgroups of $\mathrm{Hol}(N)$ are given by $J \rtimes A$, where J is a regular subgroup of $\mathrm{Hol}(N)$ and A is some subgroup of $\mathrm{Aut}(N)$ which normalises J.In total:

$$2^{m-3}\sigma_0(s)\left[4\Sigma_m + (m-2)\Sigma_{m-1}\right] + 2^{m-2}\left(\sum_{k=0}^{m-1}\prod_{i=1}^{m-1-k}\frac{2^{i+k}-1}{2^i-1}\right)$$

isomorphism types of permutation groups G of degree n which are realised by a Hopf-Galois structure of cyclic type.

The regular subgroups of $\mathrm{Hol}(N)$ are of the form

$$\langle \sigma_1, [\sigma_2, \alpha_1^{t_1}], \cdots, [\sigma_l, \alpha_{m-1}^{t_{m-1}}] \rangle$$

where all but possibly one t_i are zero, and in the case that $t_j \neq 0$, we have $1 \leq t_j \leq p_{j+1} - 1$.All transitive subgroups of $\mathrm{Hol}(N)$ are given by $J \rtimes A$, where J is a regular subgroup of $\mathrm{Hol}(N)$ and A is some subgroup of $\mathrm{Aut}(N)$ which normalises J.In total:

$$2^{m-3}\sigma_0(s)\left[4\Sigma_m + (m-2)\Sigma_{m-1}\right] + 2^{m-2}\left(\sum_{k=0}^{m-1}\prod_{i=1}^{m-1-k}\frac{2^{i+k}-1}{2^i-1}\right)$$

isomorphism types of permutation groups G of degree n which are realised by a Hopf-Galois structure of cyclic type. Each isomorphism type has a unique such Hopf-Galois structure, unless for $J \cong N_i$ for some i, we have $J \rtimes A$, where $A \cap \mathrm{Aut}(\langle \sigma_{p_i} \rangle) = \{1\}$; in which case, there are p_i Hopf-Galois structures.

For N_i, we see that $\mathrm{Hol}(N_i) \cong \mathrm{Hol}(C_{n/p_i p_{i+1}}) \times \mathrm{Hol}(C_{p_i} \rtimes C_{p_{i+1}})$. We can therefore rely on the above theory for $\mathrm{Hol}(C_{n/p_i p_{i+1}})$, and on [BML22] for $\mathrm{Hol}(C_{p_i} \rtimes C_{p_{i+1}})$.

For N_i, we see that $\mathrm{Hol}(N_i) \cong \mathrm{Hol}(C_{n/p_i p_{i+1}}) \times \mathrm{Hol}(C_{p_i} \rtimes C_{p_{i+1}})$. We can therefore rely on the above theory for $\mathrm{Hol}(C_{n/p_i p_{i+1}})$, and on [BML22] for $\mathrm{Hol}(C_{p_i} \rtimes C_{p_{i+1}})$.

The main challenge is making sure **all** transitive subgroups are found, as there are transitive subgroups of $\mathrm{Hol}(N_i)$ which aren't of the form $M_1 \times M_2$ where M_1, M_2 respectively are transitive subgroups of the two factors of $\mathrm{Hol}(N)$, and then deciding when groups are isomorphic as permutation groups.

For N_i, we see that $\mathrm{Hol}(N_i) \cong \mathrm{Hol}(C_{n/p_i p_{i+1}}) \times \mathrm{Hol}(C_{p_i} \rtimes C_{p_{i+1}})$. We can therefore rely on the above theory for $\mathrm{Hol}(C_{n/p_i p_{i+1}})$, and on [BML22] for $\mathrm{Hol}(C_{p_i} \rtimes C_{p_{i+1}})$.

The main challenge is making sure **all** transitive subgroups are found, as there are transitive subgroups of $\mathrm{Hol}(N_i)$ which aren't of the form $M_1 \times M_2$ where M_1, M_2 respectively are transitive subgroups of the two factors of $\mathrm{Hol}(N)$, and then deciding when groups are isomorphic as permutation groups.

The subgroups of interest are the 2-groups and the p_i-groups...

Conclusion and future

- The computations for the general length m Cunningham chains work are still underway, but they look to be very doable.

Conclusion and future

- The computations for the general length m Cunningham chains work are still underway, but they look to be very doable.
- The $m = 3$ case has been fully computed, and isn't that much of a specialisation from the general m work.

Conclusion and future

- The computations for the general length m Cunningham chains work are still underway, but they look to be very doable.
- The $m = 3$ case has been fully computed, and isn't that much of a specialisation from the general m work.
- There is a lot more work to be done on the general pqr case, and it is not currently known how much is actually feasible to write down or how much we can treat different groups in a single discussion (like in the Cunningham chains work).

Conclusion and future

- The computations for the general length m Cunningham chains work are still underway, but they look to be very doable.
- The $m = 3$ case has been fully computed, and isn't that much of a specialisation from the general m work.
- There is a lot more work to be done on the general pqr case, and it is not currently known how much is actually feasible to write down or how much we can treat different groups in a single discussion (like in the Cunningham chains work).
- A good next step to the majority of these is to work out the index n subgroups and look at Hopf-Galois structures on the intermediate extensions.

- Ali A. Alabdali and Nigel P. Byott, *Hopf-Galois structures of squarefree degree*, J. Algebra **559** (2020), 58–86. MR 4093704
- Nigel P. Byott and Isabel Martin-Lyons, *Hopf-Galois structures on non-normal extensions of degree related to Sophie Germain primes*, J. Pure Appl. Algebra **226** (2022), no. 3, Paper No. 106869. MR 4295182
- N. P. Byott, *Uniqueness of Hopf Galois structure for separable field extensions*, Comm. Algebra **24** (1996), no. 10, 3217–3228. MR 1402555
- Teresa Crespo and Marta Salguero, *Computation of Hopf Galois structures on low degree separable extensions and classification of those for degrees p^2 and $2p$*, Publ. Mat. **64** (2020), no. 1, 121–141. MR 4047559
- Cornelius Greither and Bodo Pareigis, *Hopf Galois theory for separable field extensions*, J. Algebra **106** (1987), no. 1, 239–258. MR 878476