Counting Hopf-Galois Structures on Galois Extensions of Squarefree Degree and Skew Braces of Squarefree Order

Nigel Byott

University of Exeter

Omaha (virtually), May 2020

(Joint work with Ali Alabdali, University of Mosul, Iraq)

Outline

Outline

1. Review of Counting Hopf-Galois Structures

Outline

1. Review of Counting Hopf-Galois Structures
2. Review of Counting Skew Braces

Outline

1. Review of Counting Hopf-Galois Structures
2. Review of Counting Skew Braces
3. Groups of Squarefree Order

Outline

1. Review of Counting Hopf-Galois Structures
2. Review of Counting Skew Braces
3. Groups of Squarefree Order
4. Result for Skew Braces of Squarefree Order

Outline

Outline

1. Review of Counting Hopf-Galois Structures
2. Review of Counting Skew Braces
3. Groups of Squarefree Order
4. Result for Skew Braces of Squarefree Order
5. Result for Hopf-Galois Structures of Squarefree Degree
6. Sketch of Proofs

Outline

Outline

1. Review of Counting Hopf-Galois Structures
2. Review of Counting Skew Braces
3. Groups of Squarefree Order
4. Result for Skew Braces of Squarefree Order
5. Result for Hopf-Galois Structures of Squarefree Degree
6. Sketch of Proofs
7. Where Next?

A.Alabdali & N.P.Byott: *Counting Hopf-Galois structures on cyclic field extensions of squarefree degree.* J. Algebra 493 (2018), 1-19
A.Alabdali & N.P.Byott: *Counting Hopf-Galois structures of squarefree degree.* J. Algebra 559 (2020), 58–86.
A.Alabdali & N.P.Byott: *Skew braces of squarefree order.* J. Algebra Appl., *to appear*.

I. Review of Counting Hopf-Galois Structures

I. Review of Counting Hopf-Galois Structures

Theorem (Greither & Pareigis, 1987)

Let L/K be a Galois extension of fields, and let $\Gamma = \mathrm{Gal}(L/K)$. Then the Hopf-Galois structures on L/K correspond bijectively to regular subgroups G of $\mathrm{Perm}(\Gamma)$ which are normalised by the group $\lambda(\Gamma)$ of left translations by Γ.

I. Review of Counting Hopf-Galois Structures

Theorem (Greither & Pareigis, 1987)

Let L/K be a Galois extension of fields, and let $\Gamma = \mathrm{Gal}(L/K)$. Then the Hopf-Galois structures on L/K correspond bijectively to regular subgroups G of $\mathrm{Perm}(\Gamma)$ which are normalised by the group $\lambda(\Gamma)$ of left translations by Γ.

Then $|G| = |\Gamma|$ but in general G and Γ need not be isomorphic. The *type* of a Hopf-Galois structure is the isomorphism type of the corresponding G.

I. Review of Counting Hopf-Galois Structures

Theorem (Greither & Pareigis, 1987)

Let L/K be a Galois extension of fields, and let $\Gamma = \mathrm{Gal}(L/K)$. Then the Hopf-Galois structures on L/K correspond bijectively to regular subgroups G of $\mathrm{Perm}(\Gamma)$ which are normalised by the group $\lambda(\Gamma)$ of left translations by Γ.

Then $|G| = |\Gamma|$ but in general G and Γ need not be isomorphic. The *type* of a Hopf-Galois structure is the isomorphism type of the corresponding G.

G is normalised by $\lambda(\Gamma) \Leftrightarrow \lambda(\Gamma) \subseteq \mathrm{Norm}_{\mathrm{Perm}(\Gamma)}(G)$ where

$$\mathrm{Norm}_{\mathrm{Perm}(\Gamma)}(G) \cong G \rtimes \mathrm{Aut}(G) =: \mathrm{Hol}(G),$$

the *holomorph* of G.

If G is as in the theorem, so is $G^{op} = \mathrm{Cent}_{\mathrm{Perm}(\Gamma)}(G)$, and

- $$G^{op} \cong G,$$

- $$G^{op} = G \Leftrightarrow G \text{ is abelian.}$$

If G is as in the theorem, so is $G^{op} = \mathrm{Cent}_{\mathrm{Perm}(\Gamma)}(G)$, and

- $$G^{op} \cong G,$$
- $$G^{op} = G \Leftrightarrow G \text{ is abelian.}$$

So Hopf-Galois structures of nonabelian type occur in pairs.

If G is as in the theorem, so is $G^{op} = \mathrm{Cent}_{\mathrm{Perm}(\Gamma)}(G)$, and

- $$G^{op} \cong G,$$
- $$G^{op} = G \Leftrightarrow G \text{ is abelian.}$$

So Hopf-Galois structures of nonabelian type occur in pairs.

For example, the right regular subgroup $\rho(\Gamma)$ gives the classical Hopf-Galois structure, and is paired with $\lambda(\Gamma)$, which gives the "canonical non-classsical Hopf-Galois structure".

We now change perspective and start with abstract groups Γ, G of the same (finite) order.

We now change perspective and start with abstract groups Γ, G of the same (finite) order.

The regular *subgroups* isomorphic to G in $\mathrm{Perm}(\Gamma)$ are the images of the regular *embeddings* $\alpha : G \hookrightarrow \mathrm{Perm}(\Gamma)$, and two regular embeddings α, α' have the same image if $\alpha' = \alpha \circ \phi$ for some $\phi \in \mathrm{Aut}(G)$.

We now change perspective and start with abstract groups Γ, G of the same (finite) order.

The regular *subgroups* isomorphic to G in $\mathrm{Perm}(\Gamma)$ are the images of the regular *embeddings* $\alpha : G \hookrightarrow \mathrm{Perm}(\Gamma)$, and two regular embeddings α, α' have the same image if $\alpha' = \alpha \circ \phi$ for some $\phi \in \mathrm{Aut}(G)$.

A regular embedding $\alpha : G \hookrightarrow \mathrm{Perm}(\Gamma)$ gives rise to a bijection

$$\hat{\alpha} : G \to \Gamma, \qquad \hat{\alpha}(g) = \alpha(g) \cdot e_\Gamma$$

and hence an isomorphism $\mathrm{Perm}(\Gamma) \to \mathrm{Perm}(G)$.

We now change perspective and start with abstract groups Γ, G of the same (finite) order.

The regular *subgroups* isomorphic to G in $\mathrm{Perm}(\Gamma)$ are the images of the regular *embeddings* $\alpha : G \hookrightarrow \mathrm{Perm}(\Gamma)$, and two regular embeddings α, α' have the same image if $\alpha' = \alpha \circ \phi$ for some $\phi \in \mathrm{Aut}(G)$.

A regular embedding $\alpha : G \hookrightarrow \mathrm{Perm}(\Gamma)$ gives rise to a bijection

$$\hat{\alpha} : G \to \Gamma, \qquad \hat{\alpha}(g) = \alpha(g) \cdot e_\Gamma$$

and hence an isomorphism $\mathrm{Perm}(\Gamma) \to \mathrm{Perm}(G)$.

Hence we get a bijection between regular embeddings $\alpha : G \hookrightarrow \mathrm{Perm}(\Gamma)$ and regular embeddings $\beta : \Gamma \to \mathrm{Perm}(G)$.

Putting this all together, if we define

$$e(\Gamma, G) := \# \text{ of Hopf-Galois structures of type } G \text{ on a } \Gamma\text{-extension}$$

then

Putting this all together, if we define

$$e(\Gamma, G) := \#\text{ of Hopf-Galois structures of type } G \text{ on a } \Gamma\text{-extension}$$

then

$$e(\Gamma, G) = \#\text{ of } \mathrm{Aut}(G)\text{-orbits of regular embeddings } \alpha : G \to \mathrm{Perm}(\Gamma) \text{ with } \alpha(G) \text{ normalised by } \lambda(\Gamma)$$

Putting this all together, if we define

$$e(\Gamma, G) := \#\text{ of Hopf-Galois structures of type } G \text{ on a } \Gamma\text{-extension}$$

then

$$\begin{aligned} e(\Gamma, G) &= \#\text{ of } \mathrm{Aut}(G)\text{-orbits of regular embeddings } \alpha : G \to \mathrm{Perm}(\Gamma) \\ &\qquad \text{with } \alpha(G) \text{ normalised by } \lambda(\Gamma) \\ &= \frac{\#\text{ of regular embeddings } \beta : \Gamma \to \mathrm{Hol}(G)}{|\mathrm{Aut}(G)|} \end{aligned}$$

Putting this all together, if we define

$$e(\Gamma, G) := \#\text{ of Hopf-Galois structures of type } G \text{ on a } \Gamma\text{-extension}$$

then

$$\begin{aligned} e(\Gamma, G) &= \#\text{ of } \mathrm{Aut}(G)\text{-orbits of regular embeddings } \alpha : G \to \mathrm{Perm}(\Gamma) \\ &\qquad \text{with } \alpha(G) \text{ normalised by } \lambda(\Gamma) \\ &= \frac{\#\text{ of regular embeddings } \beta : \Gamma \to \mathrm{Hol}(G)}{|\mathrm{Aut}(G)|} \\ &= \frac{|\mathrm{Aut}(\Gamma)|}{|\mathrm{Aut}(G)|} \times \#\text{ of regular subgroups in } \mathrm{Hol}(G) \text{ isomorphic to } \Gamma. \end{aligned}$$

Putting this all together, if we define

$$e(\Gamma, G) := \#\text{ of Hopf-Galois structures of type } G \text{ on a } \Gamma\text{-extension}$$

then

$$\begin{aligned} e(\Gamma, G) &= \#\text{ of } \mathrm{Aut}(G)\text{-orbits of regular embeddings } \alpha : G \to \mathrm{Perm}(\Gamma) \\ &\qquad \text{with } \alpha(G) \text{ normalised by } \lambda(\Gamma) \\ &= \frac{\#\text{ of regular embeddings } \beta : \Gamma \to \mathrm{Hol}(G)}{|\mathrm{Aut}(G)|} \\ &= \frac{|\mathrm{Aut}(\Gamma)|}{|\mathrm{Aut}(G)|} \times \#\text{ of regular subgroups in } \mathrm{Hol}(G) \text{ isomorphic to } \Gamma. \end{aligned}$$

So, to count the Hopf-Galois structures of type G on a field extension with Galois group Γ, it suffices to look for regular subgroups in $\mathrm{Hol}(G)$, which is much smaller group than $\mathrm{Perm}(\Gamma)$.

II. Review of Counting Skew Braces

Definition

A (left) **skew brace** $(B, +, *)$ *is a set* B *with binary operations* $+$, $*$ *such that*

II. Review of Counting Skew Braces

Definition

A (left) **skew brace** $(B, +, *)$ *is a set B with binary operations* $+$, $*$ *such that*

- $(B, +)$ *is a group (the* **additive group** *of B);*

II. Review of Counting Skew Braces

Definition

A (left) **skew brace** $(B, +, *)$ *is a set* B *with binary operations* $+$, $*$ *such that*

- $(B, +)$ *is a group (the* **additive group** *of* B*);*
- $(B, *)$ *is a group (the* **multiplicative group** *of* B*);*

II. Review of Counting Skew Braces

Definition

A (left) **skew brace** $(B, +, *)$ *is a set* B *with binary operations* $+$, $*$ *such that*

- $(B, +)$ *is a group (the* **additive group** *of* B*);*
- $(B, *)$ *is a group (the* **multiplicative group** *of* B*);*
- $a * (b + c) = a * b - a + a * c \; \forall a, b, c \in B$.

II. Review of Counting Skew Braces

Definition

A (left) **skew brace** $(B, +, *)$ *is a set* B *with binary operations* $+$, $*$ *such that*

- $(B, +)$ *is a group (the* **additive group** *of* B*);*
- $(B, *)$ *is a group (the* **multiplicative group** *of* B*);*
- $a * (b + c) = a * b - a + a * c \; \forall a, b, c \in B$.

$(B, +, *)$ *is a* **brace** *if* $(B, +)$ *is abelian.*

II. Review of Counting Skew Braces

Definition

A (left) **skew brace** $(B, +, *)$ *is a set* B *with binary operations* $+$, $*$ *such that*

- $(B, +)$ *is a group (the* **additive group** *of* B*);*
- $(B, *)$ *is a group (the* **multiplicative group** *of* B*);*
- $a * (b + c) = a * b - a + a * c \ \forall a, b, c \in B.$

$(B, +, *)$ *is a* **brace** *if* $(B, +)$ *is abelian.*

Braces were introduced by Rump (2007) to study non-degenerate involutive set-theoretical solutions of the Yang-Baxter Equation (YBE).

II. Review of Counting Skew Braces

Definition

A (left) **skew brace** $(B, +, *)$ *is a set* B *with binary operations* $+$, $*$ *such that*

- $(B, +)$ *is a group (the* **additive group** *of* B*);*
- $(B, *)$ *is a group (the* **multiplicative group** *of* B*);*
- $a * (b + c) = a * b - a + a * c \ \forall a, b, c \in B.$

$(B, +, *)$ *is a* **brace** *if* $(B, +)$ *is abelian.*

Braces were introduced by Rump (2007) to study non-degenerate involutive set-theoretical solutions of the Yang-Baxter Equation (YBE).

They were generalised to skew braces by Guarnieri & Vendramin (2017).

II. Review of Counting Skew Braces

Definition

A (left) **skew brace** $(B, +, *)$ *is a set* B *with binary operations* $+$, $*$ *such that*

- $(B, +)$ *is a group (the* **additive group** *of* B*);*
- $(B, *)$ *is a group (the* **multiplicative group** *of* B*);*
- $a * (b + c) = a * b - a + a * c \; \forall a, b, c \in B$.

$(B, +, *)$ *is a* **brace** *if* $(B, +)$ *is abelian.*

Braces were introduced by Rump (2007) to study non-degenerate involutive set-theoretical solutions of the Yang-Baxter Equation (YBE).

They were generalised to skew braces by Guarnieri & Vendramin (2017).

Skew braces give non-involutive solutions to YBE.

If $(B, +, *)$ is a skew brace, then $(B, *)$ acts on $(B, +)$ via

$$\lambda : (B, *) \to \mathrm{Aut}(B, +), \qquad b \mapsto \lambda_b \text{ with } \lambda_b(a) = -b + b * a.$$

If $(B, +, *)$ is a skew brace, then $(B, *)$ acts on $(B, +)$ via

$$\lambda : (B, *) \to \mathrm{Aut}(B, +), \qquad b \mapsto \lambda_b \text{ with } \lambda_b(a) = -b + b * a.$$

Then the set -theoretic map

$$B \to B \times \mathrm{Aut}(B, +), \qquad b \mapsto (b, \lambda_b)$$

gives a regular embedding $(B, *) \to \mathrm{Hol}(B, +) = (B, +) \rtimes \mathrm{Aut}(B, +)$.

If $(B, +, *)$ is a skew brace, then $(B, *)$ acts on $(B, +)$ via

$$\lambda : (B, *) \to \mathrm{Aut}(B, +), \qquad b \mapsto \lambda_b \text{ with } \lambda_b(a) = -b + b * a.$$

Then the set -theoretic map

$$B \to B \times \mathrm{Aut}(B, +), \qquad b \mapsto (b, \lambda_b)$$

gives a regular embedding $(B, *) \to \mathrm{Hol}(B, +) = (B, +) \rtimes \mathrm{Aut}(B, +)$.

Conversely, given groups M, A, we can decompose a regular embedding $M \to \mathrm{Hol}(A)$ into a homomorphism $M \to Aut(A)$ and a bijection $M \to A$, whch fit together to form a skew brace $(B, +, *)$ with $(B, +) \cong A$ and $(B, *) \cong M$. Composing the embedding with an element of $\mathrm{Aut}(M)$ or of $\mathrm{Aut}(A)$ will not change the isomorphism type of the skew brace.

If $(B, +, *)$ is a skew brace, then $(B, *)$ acts on $(B, +)$ via

$$\lambda : (B, *) \to \mathrm{Aut}(B, +), \qquad b \mapsto \lambda_b \text{ with } \lambda_b(a) = -b + b * a.$$

Then the set -theoretic map

$$B \to B \times \mathrm{Aut}(B, +), \qquad b \mapsto (b, \lambda_b)$$

gives a regular embedding $(B, *) \to \mathrm{Hol}(B, +) = (B, +) \rtimes \mathrm{Aut}(B, +)$.

Conversely, given groups M, A, we can decompose a regular embedding $M \to \mathrm{Hol}(A)$ into a homomorphism $M \to Aut(A)$ and a bijection $M \to A$, whch fit together to form a skew brace $(B, +, *)$ with $(B, +) \cong A$ and $(B, *) \cong M$. Composing the embedding with an element of $\mathrm{Aut}(M)$ or of $\mathrm{Aut}(A)$ will not change the isomorphism type of the skew brace.

Let $b(M, A)$ denote the number of skew braces (up to isomorphism) with multiplicative group isomorphic to M and additive group isomorphic to A.

If $(B, +, *)$ is a skew brace, then $(B, *)$ acts on $(B, +)$ via

$$\lambda : (B, *) \to \mathrm{Aut}(B, +), \qquad b \mapsto \lambda_b \text{ with } \lambda_b(a) = -b + b * a.$$

Then the set -theoretic map

$$B \to B \times \mathrm{Aut}(B, +), \qquad b \mapsto (b, \lambda_b)$$

gives a regular embedding $(B, *) \to \mathrm{Hol}(B, +) = (B, +) \rtimes \mathrm{Aut}(B, +)$.

Conversely, given groups M, A, we can decompose a regular embedding $M \to \mathrm{Hol}(A)$ into a homomorphism $M \to Aut(A)$ and a bijection $M \to A$, whch fit together to form a skew brace $(B, +, *)$ with $(B, +) \cong A$ and $(B, *) \cong M$. Composing the embedding with an element of $\mathrm{Aut}(M)$ or of $\mathrm{Aut}(A)$ will not change the isomorphism type of the skew brace.

Let $b(M, A)$ denote the number of skew braces (up to isomorphism) with multiplicative group isomorphic to M and additive group isomorphic to A.

Then $b(M, A)$ is the number of $(\mathrm{Aut}(M) \times \mathrm{Aut}(A))$-orbits of regular embeddings $M \to \mathrm{Hol}(A)$.

Summmary so far:

$$e(\Gamma, G) \quad = \quad \# \text{ of } \mathrm{Aut}(G)\text{-orbits of regular embeddings } \Gamma \to \mathrm{Hol}(G)$$

Summmary so far:

$$e(\Gamma, G) = \#\text{ of } \mathrm{Aut}(G)\text{-orbits of regular embeddings } \Gamma \to \mathrm{Hol}(G)$$
$$= \frac{|\mathrm{Aut}(\Gamma)|}{|\mathrm{Aut}(G)|} \times \#\text{ of regular subgroups in } \mathrm{Hol}(G) \text{ isomorphic to } \Gamma,$$

Summmary so far:

$$e(\Gamma, G) = \# \text{ of } \mathrm{Aut}(G)\text{-orbits of regular embeddings } \Gamma \to \mathrm{Hol}(G)$$
$$= \frac{|\mathrm{Aut}(\Gamma)|}{|\mathrm{Aut}(G)|} \times \# \text{ of regular subgroups in } \mathrm{Hol}(G) \text{ isomorphic to } \Gamma,$$

while

$$b(\Gamma, G) = \# \text{ of } \mathrm{Aut}(\Gamma) \times \mathrm{Aut}(G)\text{-orbits of regular embeddings } \Gamma \to \mathrm{Hol}(G)$$

Summmary so far:

$$\begin{aligned} e(\Gamma, G) &= \#\text{ of } \mathrm{Aut}(G)\text{-orbits of regular embeddings } \Gamma \to \mathrm{Hol}(G) \\ &= \frac{|\mathrm{Aut}(\Gamma)|}{|\mathrm{Aut}(G)|} \times \#\text{ of regular subgroups in } \mathrm{Hol}(G) \text{ isomorphic to } \Gamma, \end{aligned}$$

while

$$\begin{aligned} b(\Gamma, G) &= \#\text{ of } \mathrm{Aut}(\Gamma) \times \mathrm{Aut}(G)\text{-orbits of regular} \\ &\qquad \text{embeddings } \Gamma \to \mathrm{Hol}(G) \\ &= \#\text{ of } \mathrm{Aut}(G)\text{-orbits of regular subgroups in } \mathrm{Hol}(G) \\ &\qquad \text{isomorphic to } \Gamma. \end{aligned}$$

Summmary so far:

$$\begin{aligned} e(\Gamma, G) &= \#\text{ of } \mathrm{Aut}(G)\text{-orbits of regular embeddings } \Gamma \to \mathrm{Hol}(G) \\ &= \frac{|\mathrm{Aut}(\Gamma)|}{|\mathrm{Aut}(G)|} \times \#\text{ of regular subgroups in } \mathrm{Hol}(G) \text{ isomorphic to } \Gamma, \end{aligned}$$

while

$$\begin{aligned} b(\Gamma, G) &= \#\text{ of } \mathrm{Aut}(\Gamma) \times \mathrm{Aut}(G)\text{-orbits of regular} \\ &\qquad \text{embeddings } \Gamma \to \mathrm{Hol}(G) \\ &= \#\text{ of } \mathrm{Aut}(G)\text{-orbits of regular subgroups in } \mathrm{Hol}(G) \\ &\qquad \text{isomorphic to } \Gamma. \end{aligned}$$

So the problems of finding $e(\Gamma, G)$ and finding $b(\Gamma, G)$ are closely related (but not equivalent).

Summmary so far:

$$e(\Gamma, G) = \#\text{ of } \mathrm{Aut}(G)\text{-orbits of regular embeddings } \Gamma \to \mathrm{Hol}(G)$$
$$= \frac{|\mathrm{Aut}(\Gamma)|}{|\mathrm{Aut}(G)|} \times \#\text{ of regular subgroups in } \mathrm{Hol}(G) \text{ isomorphic to } \Gamma,$$

while

$$b(\Gamma, G) = \#\text{ of } \mathrm{Aut}(\Gamma) \times \mathrm{Aut}(G)\text{-orbits of regular embeddings } \Gamma \to \mathrm{Hol}(G)$$
$$= \#\text{ of } \mathrm{Aut}(G)\text{-orbits of regular subgroups in } \mathrm{Hol}(G) \text{ isomorphic to } \Gamma.$$

So the problems of finding $e(\Gamma, G)$ and finding $b(\Gamma, G)$ are closely related (but not equivalent).

Each of the groups $\mathrm{Aut}(\Gamma)$ and $\mathrm{Aut}(G)$ acts freely on the set of regular embeddings (so all orbits have the same size), but $\mathrm{Aut}(\Gamma) \times \mathrm{Aut}(G)$ does not act freely, and its orbits may have different sizes.

III. Groups of squarefree order

Let n be squarefree. If G is a group of order n, then all Sylow subgroups of G are cyclic, so G is metabelian.

III. Groups of squarefree order

Let n be squarefree. If G is a group of order n, then all Sylow subgroups of G are cyclic, so G is metabelian.
In fact

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

where $de = n$ and $ord_e(k) = d$.

III. Groups of squarefree order

Let n be squarefree. If G is a group of order n, then all Sylow subgroups of G are cyclic, so G is metabelian.
In fact

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

where $de = n$ and $ord_e(k) = d$.

We have $G(d, e, k) \cong G(d', e', k')$ if and only if

- $d = d'$,

III. Groups of squarefree order

Let n be squarefree. If G is a group of order n, then all Sylow subgroups of G are cyclic, so G is metabelian.
In fact

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

where $de = n$ and $ord_e(k) = d$.

We have $G(d,e,k) \cong G(d',e',k')$ if and only if

- $d = d'$,
- $e = e'$, and

III. Groups of squarefree order

Let n be squarefree. If G is a group of order n, then all Sylow subgroups of G are cyclic, so G is metabelian.
In fact

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

where $de = n$ and $ord_e(k) = d$.

We have $G(d, e, k) \cong G(d', e', k')$ if and only if

- $d = d'$,
- $e = e'$, and
- k, k' generate the same cyclic subgroup of order d in $\mathbb{Z}_e^\times$.

III. Groups of squarefree order

Let n be squarefree. If G is a group of order n, then all Sylow subgroups of G are cyclic, so G is metabelian.
In fact

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

where $de = n$ and $ord_e(k) = d$.

We have $G(d,e,k) \cong G(d',e',k')$ if and only if

- $d = d'$,
- $e = e'$, and
- k, k' generate the same cyclic subgroup of order d in $\mathbb{Z}_e^\times$.

Let

$$z = \gcd(e, k-1), \qquad g = e/z.$$

III. Groups of squarefree order

Let n be squarefree. If G is a group of order n, then all Sylow subgroups of G are cyclic, so G is metabelian.
In fact

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

where $de = n$ and $ord_e(k) = d$.

We have $G(d, e, k) \cong G(d', e', k')$ if and only if

- $d = d'$,
- $e = e'$, and
- k, k' generate the same cyclic subgroup of order d in $\mathbb{Z}_e^\times$.

Let

$$z = \gcd(e, k-1), \qquad g = e/z.$$

Then the centre of G is cyclic of order z, and the commutator subgroup of G is cyclic of order g.

The primes p dividing n are of 3 kinds:

The primes p dividing n are of 3 kinds:

- $p \mid z$, i.e. p is "central";

The primes p dividing n are of 3 kinds:

- $p \mid z$, i.e. p is "central";
- $p \mid g$, i.e. p is "acted on";

The primes p dividing n are of 3 kinds:

- $p \mid z$, i.e. p is "central";
- $p \mid g$, i.e. p is "acted on";
- $p \mid d$, i.e. p "acts".

The primes p dividing n are of 3 kinds:

- $p \mid z$, i.e. p is "central";
- $p \mid g$, i.e. p is "acted on";
- $p \mid d$, i.e. p "acts".

The primes p dividing n are of 3 kinds:

- $p \mid z$, i.e. p is "central";
- $p \mid g$, i.e. p is "acted on";
- $p \mid d$, i.e. p "acts".

We have

- Coarse invariants for G: the factors z, g, d of n;

The primes p dividing n are of 3 kinds:

- $p \mid z$, i.e. p is "central";
- $p \mid g$, i.e. p is "acted on";
- $p \mid d$, i.e. p "acts".

We have

- Coarse invariants for G: the factors z, g, d of n;
- Finer invariants for G: $r_q = \mathrm{ord}_q(k)$ for each prime $q \mid e$, which satisfy

$$r_q = 1 \Leftrightarrow q \mid z, \qquad r_q \mid \gcd(d, q-1), \qquad \mathrm{lcm}_{q|e}\{r_q\} = d.$$

The primes p dividing n are of 3 kinds:

- $p \mid z$, i.e. p is "central";
- $p \mid g$, i.e. p is "acted on";
- $p \mid d$, i.e. p "acts".

We have

- Coarse invariants for G: the factors z, g, d of n;
- Finer invariants for G: $r_q = \mathrm{ord}_q(k)$ for each prime $q \mid e$, which satisfy

$$r_q = 1 \Leftrightarrow q \mid z, \qquad r_q \mid \gcd(d, q-1), \qquad \mathrm{lcm}_{q|e}\{r_q\} = d.$$

- Complete invariants for G are $e = gz$ and the group $\langle k \rangle \subseteq \mathbb{Z}_e^\times$.

Example

$n = 2 \cdot 3 \cdot 7 \cdot 13$, $d = 6$, $e = 91$.

Here $G_1 \cong G_2$*, but no two of* G_2, G_3, G_4, G_5 *are isomorphic.*

	k	k mod 7	k mod 13	r_7	r_{13}	g	z
G_1	3	3	3	6	3	91	1
G_2	61	5	9	6	3	91	1
G_3	87	3	9	6	3	91	1
G_4	51	2	12	3	2	91	1
G_5	36	1	10	1	6	13	7

IV. Result for Skew Braces of Squarefree Order

Let n be squarefree, and consider two groups of order n:

$$G := G(d, e, k), \qquad \Gamma := G(\delta, \varepsilon, \kappa).$$

IV. Result for Skew Braces of Squarefree Order

Let n be squarefree, and consider two groups of order n:

$$G := G(d, e, k), \qquad \Gamma := G(\delta, \varepsilon, \kappa).$$

Our result for skew braces is easy to state as it depends only on the coarse invariants for G and Γ,

$$z = \gcd(e, k-1), \quad g = e/z; \qquad \zeta = \gcd(\varepsilon, \kappa - 1), \quad \gamma = \varepsilon/\zeta,$$

together with a quantity linking the two groups:

$$w = \varphi(\gcd(d, \delta)).$$

IV. Result for Skew Braces of Squarefree Order

Let n be squarefree, and consider two groups of order n:

$$G := G(d, e, k), \qquad \Gamma := G(\delta, \varepsilon, \kappa).$$

Our result for skew braces is easy to state as it depends only on the coarse invariants for G and Γ,

$$z = \gcd(e, k-1), \quad g = e/z; \qquad \zeta = \gcd(\varepsilon, \kappa - 1), \quad \gamma = \varepsilon/\zeta,$$

together with a quantity linking the two groups:

$$w = \varphi(\gcd(d, \delta)).$$

Theorem 1 (Alabdali + B.)

$$b(\Gamma, G) = \begin{cases} 2^{\omega(g)} w & \text{if } \gamma \mid e, \\ 0 & \text{if } \gamma \nmid e; \end{cases}$$

where $\omega(g)$ is the number of (distinct) primes dividing g.

On the basis of extensive computations, Bardakov, Neshchadim & Yadav (Int. J. Algebra Comput., *to appear*) made the

Conjecture

On the basis of extensive computations, Bardakov, Neshchadim & Yadav (Int. J. Algebra Comput., *to appear*) made the

Conjecture

For primes $q > p \geq 3$:

(i) *the number of isomorphism classes of braces of order $2pq$ is*

$$\begin{cases} 4 & \text{if } p \nmid (q-1), \\ 6 & \text{if } p \mid (q-1); \end{cases}$$

On the basis of extensive computations, Bardakov, Neshchadim & Yadav (Int. J. Algebra Comput., *to appear*) made the

Conjecture

For primes $q > p \geq 3$:

(i) *the number of isomorphism classes of braces of order $2pq$ is*

$$\begin{cases} 4 & \text{if } p \nmid (q-1), \\ 6 & \text{if } p \mid (q-1); \end{cases}$$

(ii) *the number of isomorphism classes of skew braces of order $2pq$ is*

$$\begin{cases} 36 & \text{if } p \nmid (q-1), \\ 8p + 54 & \text{if } p \mid (q-1); \end{cases}$$

On the basis of extensive computations, Bardakov, Neshchadim & Yadav (Int. J. Algebra Comput., *to appear*) made the

Conjecture

For primes $q > p \geq 3$:

(i) *the number of isomorphism classes of braces of order $2pq$ is*

$$\begin{cases} 4 & \text{if } p \nmid (q-1), \\ 6 & \text{if } p \mid (q-1); \end{cases}$$

(ii) *the number of isomorphism classes of skew braces of order $2pq$ is*

$$\begin{cases} 36 & \text{if } p \nmid (q-1), \\ 8p+54 & \text{if } p \mid (q-1); \end{cases}$$

It follows from Theorem 1 that **this Conjecture is true**.

Intuition for the factor $2^{\omega(g)}$

Recall that

$$b(\Gamma, G) = 2^{\omega(g)} w \text{ if } \gamma \mid e.$$

Intuition for the factor $2^{\omega(g)}$

Recall that

$$b(\Gamma, G) = 2^{\omega(g)} w \text{ if } \gamma \mid e.$$

Consider the special case

$$\Gamma \cong G \cong D_{2q_1 \cdots q_t}$$

where $q_1, \ldots, q_t$ are distinct odd primes. Here $g = e = \gamma = q_1 \cdots q_t$ and $d = \delta = 2$, so that $w = \varphi(\gcd(d, \delta)) = 1$ and $\omega(g) = t$.

Intuition for the factor $2^{\omega(g)}$

Recall that

$$b(\Gamma, G) = 2^{\omega(g)} w \text{ if } \gamma \mid e.$$

Consider the special case

$$\Gamma \cong G \cong D_{2q_1 \cdots q_t}$$

where $q_1, \ldots, q_t$ are distinct odd primes. Here $g = e = \gamma = q_1 \cdots q_t$ and $d = \delta = 2$, so that $w = \varphi(\gcd(d, \delta)) = 1$ and $\omega(g) = t$.

We are interested in regular embeddings $\Gamma \to \mathrm{Hol}(G)$. If $\sigma_1, \ldots, \sigma_t \in \Gamma$ have order q_1, ..., q_t respectively, we can embed each σ_i into $\mathrm{Hol}(G)$ as either $\lambda(\sigma_i)$ or $\rho(\sigma_i)$.

Intuition for the factor $2^{\omega(g)}$

Recall that

$$b(\Gamma, G) = 2^{\omega(g)} w \text{ if } \gamma \mid e.$$

Consider the special case

$$\Gamma \cong G \cong D_{2q_1 \cdots q_t}$$

where $q_1, \ldots, q_t$ are distinct odd primes. Here $g = e = \gamma = q_1 \cdots q_t$ and $d = \delta = 2$, so that $w = \varphi(\gcd(d, \delta)) = 1$ and $\omega(g) = t$.

We are interested in regular embeddings $\Gamma \to \mathrm{Hol}(G)$. If $\sigma_1, \ldots, \sigma_t \in \Gamma$ have order $q_1, \ldots, q_t$ respectively, we can embed each σ_i into $\mathrm{Hol}(G)$ as either $\lambda(\sigma_i)$ or $\rho(\sigma_i)$.

This gives us $2^t = 2^{\omega(g)}$ distinct regular subgroups of $\mathrm{Hol}(G)$ isomorphic to $D_{2q_1 \cdots q_t}$, each of which corresponds to one Hopf-Galois structure and one isomorphism class of skew braces.

Intuition for the factor $2^{\omega(g)}$

Recall that

$$b(\Gamma, G) = 2^{\omega(g)} w \text{ if } \gamma \mid e.$$

Consider the special case

$$\Gamma \cong G \cong D_{2q_1 \cdots q_t}$$

where $q_1, \ldots, q_t$ are distinct odd primes. Here $g = e = \gamma = q_1 \cdots q_t$ and $d = \delta = 2$, so that $w = \varphi(\gcd(d, \delta)) = 1$ and $\omega(g) = t$.

We are interested in regular embeddings $\Gamma \to \mathrm{Hol}(G)$. If $\sigma_1, \ldots, \sigma_t \in \Gamma$ have order q_1, ..., q_t respectively, we can embed each σ_i into $\mathrm{Hol}(G)$ as either $\lambda(\sigma_i)$ or $\rho(\sigma_i)$.

This gives us $2^t = 2^{\omega(g)}$ distinct regular subgroups of $\mathrm{Hol}(G)$ isomorphic to $D_{2q_1 \cdots q_t}$, each of which corresponds to one Hopf-Galois structure and one isomorphism class of skew braces.

In general, for each prime $q \mid g$ separately, there seems to be a "$G \leftrightarrow G^{op}$ pairing" for the Sylow q-subgroup of G. This explains the factor $2^{\omega(g)}$.

Intuition for the factor w

Our strategy is to regard

$$G = \langle \sigma, \tau : \sigma^e = 1 = \tau^d, \tau\sigma\tau^{-1} = \tau^k \rangle,$$

as fixed once and for all, and look for regular subgroups of $\mathrm{Hol}(G)$ isomorphic to Γ. These only exist if $\gamma \mid e$.

Intuition for the factor w

Our strategy is to regard

$$G = \langle \sigma, \tau : \sigma^e = 1 = \tau^d, \tau\sigma\tau^{-1} = \tau^k \rangle,$$

as fixed once and for all, and look for regular subgroups of $\mathrm{Hol}(G)$ isomorphic to Γ. These only exist if $\gamma \mid e$.

We choose an alternative presentation for Γ:

$$\Gamma = G(\delta, \epsilon, \kappa) = \langle X, Y : X^\gamma = 1 = Y^{\zeta\delta}, YXY^{-1} = X^\kappa \rangle.$$

Intuition for the factor w

Our strategy is to regard

$$G = \langle \sigma, \tau : \sigma^e = 1 = \tau^d, \tau\sigma\tau^{-1} = \tau^k \rangle,$$

as fixed once and for all, and look for regular subgroups of $\mathrm{Hol}(G)$ isomorphic to Γ. These only exist if $\gamma \mid e$.

We choose an alternative presentation for Γ:

$$\Gamma = G(\delta, \epsilon, \kappa) = \langle X, Y : X^\gamma = 1 = Y^{\zeta\delta}, YXY^{-1} = X^\kappa \rangle.$$

We can take as generators of our regular subgroups elements of the form

$$X = [\sigma^a, \psi], \quad Y = [\sigma^u\tau, \psi'] \in \mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G),$$

with ψ, $\psi' \in \mathrm{Aut}(G)$ (note τ occurs in Y with exponent 1), *at the expense of* replacing κ by another element of

$$\mathcal{K} = \{\kappa^r : r \in \mathbb{Z}_\delta^\times\}.$$

Replacing Y by Y^r, and κ by κ^r, gives a new Y of the right form provided that $r \equiv 1 \pmod{d}$.

Replacing Y by Y^r, and κ by κ^r, gives a new Y of the right form provided that $r \equiv 1 \pmod{d}$.

So we are interested in the orbits on $\mathcal{K}$ of the group

$$\Delta := \{r \in \mathbb{Z}_\delta^\times : r \equiv 1 \pmod{\gcd(d, \delta)}\}.$$

Replacing Y by Y^r, and κ by κ^r, gives a new Y of the right form provided that $r \equiv 1 \pmod{d}$.

So we are interested in the orbits on $\mathcal{K}$ of the group

$$\Delta := \{r \in \mathbb{Z}_\delta^\times : r \equiv 1 \pmod{\gcd(d, \delta)}\}.$$

There are $w = \varphi(\gcd(d, \delta))$ orbits.

Replacing Y by Y^r, and κ by κ^r, gives a new Y of the right form provided that $r \equiv 1 \pmod{d}$.

So we are interested in the orbits on $\mathcal{K}$ of the group

$$\Delta := \{r \in \mathbb{Z}_\delta^\times : r \equiv 1 \pmod{\gcd(d, \delta)}\}.$$

There are $w = \varphi(\gcd(d, \delta))$ orbits.

This gives us w families $\mathcal{F}_1$, ..., $\mathcal{F}_w$ of regular subgroups, corresponding to orbit representatives $\kappa_1, \ldots, \kappa_w$.

V. Result for Hopf-Galois Structures of Squarefree Degree

Recall $r_q = \mathrm{ord}_q(k)$ for primes $q \mid e$. Similarly, let $\rho_q = \mathrm{ord}_q(\kappa)$ for $q \mid \epsilon$.

V. Result for Hopf-Galois Structures of Squarefree Degree

Recall $r_q = \mathrm{ord}_q(k)$ for primes $q \mid e$. Similarly, let $\rho_q = \mathrm{ord}_q(\kappa)$ for $q \mid \epsilon$. Then let

$$S = \{\text{primes } q \mid \gcd(g, \gamma) : \rho_q = r_q > 2\},$$
$$T = \{\text{primes } q \mid \gcd(g, \gamma) : \rho_q = r_q = 2\}.$$

V. Result for Hopf-Galois Structures of Squarefree Degree

Recall $r_q = \mathrm{ord}_q(k)$ for primes $q \mid e$. Similarly, let $\rho_q = \mathrm{ord}_q(\kappa)$ for $q \mid \epsilon$.

Then let

$$S = \{\text{primes } q \mid \gcd(g, \gamma) : \rho_q = r_q > 2\},$$
$$T = \{\text{primes } q \mid \gcd(g, \gamma) : \rho_q = r_q = 2\}.$$

For $1 \leq h \leq w$, let

$$S_h^+ = \{q \in S : \kappa_h \equiv k \pmod{q}\},$$
$$S_h^- = \{q \in S : \kappa_h \equiv k^{-1} \pmod{q}\},$$
$$S_h = S_h^+ \cup S_h^-.$$

V. Result for Hopf-Galois Structures of Squarefree Degree

Recall $r_q = \mathrm{ord}_q(k)$ for primes $q \mid e$. Similarly, let $\rho_q = \mathrm{ord}_q(\kappa)$ for $q \mid \epsilon$. Then let

$$S = \{\text{primes } q \mid \gcd(g, \gamma) : \rho_q = r_q > 2\},$$
$$T = \{\text{primes } q \mid \gcd(g, \gamma) : \rho_q = r_q = 2\}.$$

For $1 \leq h \leq w$, let

$$S_h^+ = \{q \in S : \kappa_h \equiv k \pmod{q}\},$$
$$S_h^- = \{q \in S : \kappa_h \equiv k^{-1} \pmod{q}\},$$
$$S_h = S_h^+ \cup S_h^-.$$

Theorem 2 (Alabdali + B.)

$$e(\Gamma, G) = \begin{cases} \dfrac{2^{\omega(g)}\varphi(d)\gamma}{w} \left(\displaystyle\prod_{q \in T} \frac{1}{q}\right) \displaystyle\sum_{h=1}^{w} \prod_{q \in S_h} \frac{q+1}{q} & \text{if } \gamma \mid e, \\ 0 & \text{if } \gamma \nmid e. \end{cases}$$

VI. Sketch of Proofs

$\mathrm{Aut}(G) \cong \mathbb{Z}_g \rtimes \mathbb{Z}_e^\times$, and it is generated by

- θ where $\theta(\sigma) = \sigma$, $\theta(\tau) = \sigma^z\tau$;
- ϕ_t for $t \in \mathbb{Z}_e^\times$, where $\phi_t(\sigma) = \sigma^t$, $\phi_t(\tau) = \tau$

VI. Sketch of Proofs

$\mathrm{Aut}(G) \cong \mathbb{Z}_g \rtimes \mathbb{Z}_e^\times$, and it is generated by

- θ where $\theta(\sigma) = \sigma$, $\theta(\tau) = \sigma^z\tau$;
- ϕ_t for $t \in \mathbb{Z}_e^\times$, where $\phi_t(\sigma) = \sigma^t$, $\phi_t(\tau) = \tau$

Any regular subgroup in $\mathrm{Hol}(G)$ in $\mathcal{F}_h$ (for $1 \leq h \leq w$) has a pair of generators

$$X = [\sigma^a, \theta^c], \quad Y = [\sigma^u\tau, \theta^v\phi_t]$$

satisfying $X^\gamma = Y^{\zeta\delta} = 1, YXY^{-1} = X^{\kappa_h}$. In fact, it contains exactly $\gamma\varphi(e)w/\varphi(\delta)$ such pairs.

VI. Sketch of Proofs

$\mathrm{Aut}(G) \cong \mathbb{Z}_g \rtimes \mathbb{Z}_e^\times$, and it is generated by

- θ where $\theta(\sigma) = \sigma$, $\theta(\tau) = \sigma^z \tau$;
- ϕ_t for $t \in \mathbb{Z}_e^\times$, where $\phi_t(\sigma) = \sigma^t$, $\phi_t(\tau) = \tau$

Any regular subgroup in $\mathrm{Hol}(G)$ in $\mathcal{F}_h$ (for $1 \leq h \leq w$) has a pair of generators

$$X = [\sigma^a, \theta^c], \quad Y = [\sigma^u \tau, \theta^v \phi_t]$$

satisfying $X^\gamma = Y^{\zeta\delta} = 1$, $YXY^{-1} = X^{\kappa_h}$. In fact, it contains exactly $\gamma\varphi(e)w/\varphi(\delta)$ such pairs.

For $1 \leq h \leq w$, let $\mathcal{N}_h$ be the set of quintuples

$$(t, a, c, u, v) \in \mathbb{Z}_e^\times \times \mathbb{Z}_e \times \mathbb{Z}_g \times \mathbb{Z}_e \times \mathbb{Z}_g$$

for which the corresponding X, $Y \in \mathrm{Hol}(G)$ generate a regular subgroup of $\mathrm{Hol}(G)$ in $\mathcal{F}_h$.

VI. Sketch of Proofs

$\mathrm{Aut}(G) \cong \mathbb{Z}_g \rtimes \mathbb{Z}_e^\times$, and it is generated by

- θ where $\theta(\sigma) = \sigma$, $\theta(\tau) = \sigma^z\tau$;
- ϕ_t for $t \in \mathbb{Z}_e^\times$, where $\phi_t(\sigma) = \sigma^t$, $\phi_t(\tau) = \tau$

Any regular subgroup in $\mathrm{Hol}(G)$ in $\mathcal{F}_h$ (for $1 \le h \le w$) has a pair of generators

$$X = [\sigma^a, \theta^c], \quad Y = [\sigma^u\tau, \theta^v\phi_t]$$

satisfying $X^\gamma = Y^{\zeta\delta} = 1$, $YXY^{-1} = X^{\kappa_h}$. In fact, it contains exactly $\gamma\varphi(e)w/\varphi(\delta)$ such pairs.

For $1 \le h \le w$, let $\mathcal{N}_h$ be the set of quintuples

$$(t, a, c, u, v) \in \mathbb{Z}_e^\times \times \mathbb{Z}_e \times \mathbb{Z}_g \times \mathbb{Z}_e \times \mathbb{Z}_g$$

for which the corresponding X, $Y \in \mathrm{Hol}(G)$ generate a regular subgroup of $\mathrm{Hol}(G)$ in $\mathcal{F}_h$.

Then

$$e(\Gamma, G) = \frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(\Gamma)|} \sum_{h=1}^{w} |\mathcal{N}_h| \times \frac{\varphi(\delta)}{\gamma\varphi(e)w}.$$

VI. Sketch of Proofs

$\mathrm{Aut}(G) \cong \mathbb{Z}_g \rtimes \mathbb{Z}_e^\times$, and it is generated by

- θ where $\theta(\sigma) = \sigma$, $\theta(\tau) = \sigma^z\tau$;
- ϕ_t for $t \in \mathbb{Z}_e^\times$, where $\phi_t(\sigma) = \sigma^t$, $\phi_t(\tau) = \tau$

Any regular subgroup in $\mathrm{Hol}(G)$ in $\mathcal{F}_h$ (for $1 \leq h \leq w$) has a pair of generators

$$X = [\sigma^a, \theta^c], \quad Y = [\sigma^u\tau, \theta^v\phi_t]$$

satisfying $X^\gamma = Y^{\zeta\delta} = 1$, $YXY^{-1} = X^{\kappa_h}$. In fact, it contains exactly $\gamma\varphi(e)w/\varphi(\delta)$ such pairs.

For $1 \leq h \leq w$, let $\mathcal{N}_h$ be the set of quintuples

$$(t, a, c, u, v) \in \mathbb{Z}_e^\times \times \mathbb{Z}_e \times \mathbb{Z}_g \times \mathbb{Z}_e \times \mathbb{Z}_g$$

for which the corresponding X, $Y \in \mathrm{Hol}(G)$ generate a regular subgroup of $\mathrm{Hol}(G)$ in $\mathcal{F}_h$.

Then

$$e(\Gamma, G) = \frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(\Gamma)|} \sum_{h=1}^{w} |\mathcal{N}_h| \times \frac{\varphi(\delta)}{\gamma\varphi(e)w}.$$

Then $(t, a, c, u, v) \in \mathcal{N}_h$ if and only if, for each prime $q \mid e$, the following congruences mod q are satisfied, where $\lambda = z^{-1}(k-1)$, $\mu = k^{-1}\lambda \in \mathbb{Z}_g^\times$.

Then $(t, a, c, u, v) \in \mathcal{N}_h$ if and only if, for each prime $q \mid e$, the following congruences mod q are satisfied, where $\lambda = z^{-1}(k-1)$, $\mu = k^{-1}\lambda \in \mathbb{Z}_g^\times$.

Primes q	t	a	u	c	v	Number
$q \mid \gcd(z, \gamma)$	κ_h	$\not\equiv 0$	arb.			$q(q-1)$
$q \mid \gcd(z, \zeta\delta)$	1	0	$\not\equiv 0$			$q-1$
$q \mid \gcd(g, \gamma)$, $q \notin S_h \cup T$	κ_h $\kappa_h k^{-1}$	$\not\equiv 0$ $\not\equiv 0$	arb. arb.	λa 0	arb. arb.	$2q^2(q-1)$
$q \in S_h^+$	κ_h $\kappa_h k^{-1} \equiv 1$	$\not\equiv 0$ $\not\equiv 0$	arb. arb.	λa 0	arb. 0	$q(q^2-1)$
$q \in S_h^-$	κ_h $\kappa_h k^{-1} \equiv \kappa^2$	$\not\equiv 0$ $\not\equiv 0$	arb. arb.	λa 0	μu arb.	$q(q^2-1)$
$q \in T$	$\kappa_h \equiv -1$ $\kappa_h k^{-1} \equiv 1$	$\not\equiv 0$ $\not\equiv 0$	arb. arb.	λa 0	μu 0	$2q(q-1)$
$q \mid \gcd(g, \zeta\delta)$	1 k^{-1}	0 0	arb. arb.	0 0	$\not\equiv 0$ $\not\equiv \mu u$	$2q(q-1)$

Then $(t, a, c, u, v) \in \mathcal{N}_h$ if and only if, for each prime $q \mid e$, the following congruences mod q are satisfied, where $\lambda = z^{-1}(k-1)$, $\mu = k^{-1}\lambda \in \mathbb{Z}_g^\times$.

Primes q	t	a	u	c	v	Number
$q \mid \gcd(z, \gamma)$	κ_h	$\not\equiv 0$	arb.			$q(q-1)$
$q \mid \gcd(z, \zeta\delta)$	1	0	$\not\equiv 0$			$q-1$
$q \mid \gcd(g, \gamma)$,	κ_h	$\not\equiv 0$	arb.	λa	arb.	$2q^2(q-1)$
$q \notin S_h \cup T$	$\kappa_h k^{-1}$	$\not\equiv 0$	arb.	0	arb.	
$q \in S_h^+$	κ_h	$\not\equiv 0$	arb.	λa	arb.	$q(q^2-1)$
	$\kappa_h k^{-1} \equiv 1$	$\not\equiv 0$	arb.	0	0	
$q \in S_h^-$	κ_h	$\not\equiv 0$	arb.	λa	μu	$q(q^2-1)$
	$\kappa_h k^{-1} \equiv \kappa^2$	$\not\equiv 0$	arb.	0	arb.	
$q \in T$	$\kappa_h \equiv -1$	$\not\equiv 0$	arb.	λa	μu	$2q(q-1)$
	$\kappa_h k^{-1} \equiv 1$	$\not\equiv 0$	arb.	0	0	
$q \mid \gcd(g, \zeta\delta)$	1	0	arb.	0	$\not\equiv 0$	$2q(q-1)$
	k^{-1}	0	arb.	0	$\not\equiv \mu u$	

Multiplying the contributions for each q, we can find $|\mathcal{N}_q|$ and hence complete the proof of Theorem 2.

To count skew braces, we need count $\mathrm{Aut}(G)$-orbits of regular subgroups of $\mathrm{Hol}(G)$.

To count skew braces, we need count $\mathrm{Aut}(G)$-orbits of regular subgroups of $\mathrm{Hol}(G)$.

Thus, for each $(t, a, c, u, v) \in \mathcal{N}_h$, we must weight the corresponding regular subgroup by $1/I(t, a, c, uv)$, where $I(t, a, c, u, v)$ is the index in $\mathrm{Aut}(G)$ of the stabiliser of the subgroup.

To count skew braces, we need count $\mathrm{Aut}(G)$-orbits of regular subgroups of $\mathrm{Hol}(G)$.

Thus, for each $(t, a, c, u, v) \in \mathcal{N}_h$, we must weight the corresponding regular subgroup by $1/I(t, a, c, uv)$, where $I(t, a, c, u, v)$ is the index in $\mathrm{Aut}(G)$ of the stabiliser of the subgroup.

$$b(\Gamma, G) = \frac{\varphi(\delta)}{\gamma\varphi(e)w} \sum_{h=1}^{w} \sum_{(t,a,c,u,v)\in\mathcal{N}_h} \frac{1}{I(t, a, c, u, v)}.$$

To count skew braces, we need count $\mathrm{Aut}(G)$-orbits of regular subgroups of $\mathrm{Hol}(G)$.

Thus, for each $(t, a, c, u, v) \in \mathcal{N}_h$, we must weight the corresponding regular subgroup by $1/I(t, a, c, uv)$, where $I(t, a, c, u, v)$ is the index in $\mathrm{Aut}(G)$ of the stabiliser of the subgroup.

$$b(\Gamma, G) = \frac{\varphi(\delta)}{\gamma\varphi(e)w} \sum_{h=1}^{w} \sum_{(t,a,c,u,v)\in\mathcal{N}_h} \frac{1}{I(t, a, c, u, v)}.$$

$I(t, a, c, u, v)$ is a product of contributions I_q for each prime $q \mid e$, but we need to partition these primes more finely than before.

Primes q	t	a	u	c	v	Index	Number
$q \mid \gcd(g, \delta)$	1	0	arb.	0	$\neq 0$	$q(q-1)$	$2q(q-1)$
	k^{-1}	0	arb.	0	$\neq \mu u$		
$q \mid \gcd(z, \delta)$	1	0	$\neq 0$			$q-1$	$q-1$
$q \mid \gcd(g, \gamma)$	κ_h	$\neq 0$	arb.	λa	arb.	q	$2q^2(q-1)$
$q \notin S_h \cup T$	$\kappa_h k^{-1}$	$\neq 0$	arb.	0	arb.		
$q \in S_h^+$, $t \equiv \kappa_h$	κ_h	$\neq 0$	arb.	λa	arb.	q	$q^2(q-1)$
$q \in S_h^+$, $t \equiv 1$	1	$\neq 0$	arb.	0	0	1	$q(q-1)$
$q \in S_h^-$, $t \equiv \kappa_h$	κ_h	$\neq 0$	arb.	λa	μu	1	$q(q-1)$
$q \in S_h^-$, $t \equiv \kappa_h k^{-1}$	$\kappa_h k^{-1}$	$\neq 0$	arb.	0	arb.	q	$q^2(q-1)$
$q \in T$	1	$\neq 0$	arb.	0	0	1	$2q(q-1)$
	-1	$\neq 0$	arb.	λa	μa		
$q \mid \gcd(z, \gamma)$	κ_h	$\neq 0$	arb.			1	$q(q-1)$
$q \mid \gcd(g, \zeta)$	1	0	arb.	0	$\neq 0$	q	$2q(q-1)$
	k^{-1}	0	arb.	0	$\neq \mu u$		
$q \mid (z, \zeta)$	1	0	$\neq 0$			1	$q-1$

If $q \in S_h^+$ then we have $q^2(q-1)$ quintuples mod q with $t \equiv \kappa_h$ and $q(q-1)$ quintuples with $t \equiv 1$, but I_q is q or 1 respectively.

If $q \in S_h^+$ then we have $q^2(q-1)$ quintuples mod q with $t \equiv \kappa_h$ and $q(q-1)$ quintuples with $t \equiv 1$, but I_q is q or 1 respectively.

Similarly for S_h^-.

If $q \in S_h^+$ then we have $q^2(q-1)$ quintuples mod q with $t \equiv \kappa_h$ and $q(q-1)$ quintuples with $t \equiv 1$, but I_q is q or 1 respectively.

Similarly for S_h^-.

Take arbitrary subsets $A \subseteq S_h^+$, $B \subseteq S_h^-$, and let $N_h(A, B)$ be the number of quintuples in $\mathcal{N}_h$ with

$$\{q \in S_h^+ : t \equiv 1 \pmod q\} = A; \qquad \{q \in S_h^- : t \equiv \kappa_h \pmod q\} = B.$$

If $q \in S_h^+$ then we have $q^2(q-1)$ quintuples mod q with $t \equiv \kappa_h$ and $q(q-1)$ quintuples with $t \equiv 1$, but I_q is q or 1 respectively.

Similarly for S_h^-.

Take arbitrary subsets $A \subseteq S_h^+$, $B \subseteq S_h^-$, and let $N_h(A,B)$ be the number of quintuples in $\mathcal{N}_h$ with

$$\{q \in S_h^+ : t \equiv 1 \pmod q\} = A; \qquad \{q \in S_h^- : t \equiv \kappa_h \pmod q\} = B.$$

Let $I_h(A,B)$ be the index of the stabiliser of each of these subgroups. Then

$$b(\Gamma, G) = \frac{\varphi(\delta)}{\gamma\varphi(e)w} \sum_{h=1}^{w} \sum_{A,B} \frac{N_h(A,B)}{I_h(A,B)}.$$

If $q \in S_h^+$ then we have $q^2(q-1)$ quintuples mod q with $t \equiv \kappa_h$ and $q(q-1)$ quintuples with $t \equiv 1$, but I_q is q or 1 respectively.

Similarly for S_h^-.

Take arbitrary subsets $A \subseteq S_h^+$, $B \subseteq S_h^-$, and let $N_h(A,B)$ be the number of quintuples in $\mathcal{N}_h$ with

$$\{q \in S_h^+ : t \equiv 1 \pmod{q}\} = A; \qquad \{q \in S_h^- : t \equiv \kappa_h \pmod{q}\} = B.$$

Let $I_h(A,B)$ be the index of the stabiliser of each of these subgroups. Then

$$b(\Gamma, G) = \frac{\varphi(\delta)}{\gamma\varphi(e)w} \sum_{h=1}^{w} \sum_{A,B} \frac{N_h(A,B)}{I_h(A,B)}.$$

The contribution of q to $N_h(A,B)/I_h(A,B)$ is $q(q-1)$ for *all* $q \in S_h^+ \cup S_h^-$ and is $2q(q-1)$ for all other $q \mid \gcd(g,\gamma)$.

If $q \in S_h^+$ then we have $q^2(q-1)$ quintuples mod q with $t \equiv \kappa_h$ and $q(q-1)$ quintuples with $t \equiv 1$, but I_q is q or 1 respectively.

Similarly for S_h^-.

Take arbitrary subsets $A \subseteq S_h^+$, $B \subseteq S_h^-$, and let $N_h(A,B)$ be the number of quintuples in $\mathcal{N}_h$ with

$$\{q \in S_h^+ : t \equiv 1 \pmod{q}\} = A; \qquad \{q \in S_h^- : t \equiv \kappa_h \pmod{q}\} = B.$$

Let $I_h(A,B)$ be the index of the stabiliser of each of these subgroups. Then

$$b(\Gamma, G) = \frac{\varphi(\delta)}{\gamma \varphi(e) w} \sum_{h=1}^{w} \sum_{A,B} \frac{N_h(A,B)}{I_h(A,B)}.$$

The contribution of q to $N_h(A,B)/I_h(A,B)$ is $q(q-1)$ for *all* $q \in S_h^+ \cup S_h^-$ and is $2q(q-1)$ for all other $q \mid \gcd(g,\gamma)$.

Summing over A and B restores the "missing" factor 2 so all primes $q \mid \gcd(g,\gamma)$ give the same contribution.

Multiplying the contributions for all $q \mid e$, and simplifying, we obtain the simple formula

$$b(\Gamma, G) = \begin{cases} 2^{\omega(g)} w & \text{if } \gamma \mid e, \\ 0 & \text{if } \gamma \nmid e; \end{cases}$$

proving Theorem 1.

VII. Where Next?

What about *non-normal* (but separable) field extensions L/K of squarefree degree n?

VII. Where Next?

What about *non-normal* (but separable) field extensions L/K of squarefree degree n?

The *type* of such an extension is still a group G of order n, and we have a classification for these.

VII. Where Next?

What about *non-normal* (but separable) field extensions L/K of squarefree degree n?

The *type* of such an extension is still a group G of order n, and we have a classification for these.

But, instead of a *Galois group* of order n, we have a transitive permutation group of degree n, namely $\Gamma = \mathrm{Gal}(E/K)$ where E is the Galois closure of L/K. In general, $|\Gamma|$ is not squarefree, and no classification of permutation groups of squarefree degree is available.

VII. Where Next?

What about *non-normal* (but separable) field extensions L/K of squarefree degree n?

The *type* of such an extension is still a group G of order n, and we have a classification for these.

But, instead of a *Galois group* of order n, we have a transitive permutation group of degree n, namely $\Gamma = \mathrm{Gal}(E/K)$ where E is the Galois closure of L/K. In general, $|\Gamma|$ is not squarefree, and no classification of permutation groups of squarefree degree is available.

However, if a Hopf-Galois structure on L/K exists then Γ still embeds in $\mathrm{Hol}(G)$ for some G of order n, so only *soluble* permutation groups Γ can arise.

Special cases may be amenable to exhaustive investigation.

The case $n = pq$ with $p = 2q + 1$ for primes $p > q \geq 3$ was examined in an LMS-funded undergraduate summer project (2019) by Isabel Martin-Lyons.

Special cases may be amenable to exhaustive investigation.

The case $n = pq$ with $p = 2q + 1$ for primes $p > q \geq 3$ was examined in an LMS-funded undergraduate summer project (2019) by Isabel Martin-Lyons.

Question

Does every separable L/K of squarefree degree n with soluble *Galois closure admit a Hopf-Galois structure?*

Special cases may be amenable to exhaustive investigation.

The case $n = pq$ with $p = 2q + 1$ for primes $p > q \geq 3$ was examined in an LMS-funded undergraduate summer project (2019) by Isabel Martin-Lyons.

Question

Does every separable L/K of squarefree degree n with soluble *Galois closure admit a Hopf-Galois structure?*

(i.e. Can every soluble transitive permutation group of squarefree degree occur as Γ?)

Thank you for listening!