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

Nigel Byott

University of Exeter

19 June 2019

Outline

Outline

1. Counting Hopf-Galois Structures

Outline

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

Outline

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

Outline

1. Counting Hopf-Galois Structures
2. Counting Skew Braces
3. Groups of Squarefree Order
4. Hopf-Galois Structures and Skew Braces of Squarefree Order (Joint with Ali Alabdali, University of Mosul, Iraq)

I. Counting Hopf-Galois Structures

I. Counting Hopf-Galois Structures

Definition

Let L/K be a finite extension of fields. A **Hopf-Galois structure** *on L/K consists of a K-Hopf algebra H acting on L and making it into an H-Galois extension of K in the sense of Chase and Sweedler (1969),*

I. Counting Hopf-Galois Structures

Definition

Let L/K be a finite extension of fields. A **Hopf-Galois structure** *on L/K consists of a K-Hopf algebra H acting on L and making it into an H-Galois extension of K in the sense of Chase and Sweedler (1969), i.e.*

(i) $h \cdot (st) = \sum_{(h)} (h_{(1)} \cdot s)(h_{(2)} \cdot t)$ *for all $h \in H$ and $s, t \in L$, where we write the comultiplication on H as $h \mapsto \sum_{(h)} h_{(1)} \otimes h_{(2)}$;*

I. Counting Hopf-Galois Structures

Definition

Let L/K be a finite extension of fields. A **Hopf-Galois structure** *on L/K consists of a K-Hopf algebra H acting on L and making it into an H-Galois extension of K in the sense of Chase and Sweedler (1969), i.e.*

(i) $h \cdot (st) = \sum_{(h)} (h_{(1)} \cdot s)(h_{(2)} \cdot t)$ *for all $h \in H$ and $s, t \in L$, where we write the comultiplication on H as* $h \mapsto \sum_{(h)} h_{(1)} \otimes h_{(2)}$*;*

(ii) $h \cdot 1 = \varepsilon(h) 1$ *for all $h \in H$, where $\varepsilon : H \to K$ is the counit of H;*

I. Counting Hopf-Galois Structures

Definition

Let L/K be a finite extension of fields. A **Hopf-Galois structure** *on L/K consists of a K-Hopf algebra H acting on L and making it into an H-Galois extension of K in the sense of Chase and Sweedler (1969), i.e.*

(i) $h \cdot (st) = \sum_{(h)} (h_{(1)} \cdot s)(h_{(2)} \cdot t)$ *for all $h \in H$ and $s, t \in L$, where we write the comultiplication on H as $h \mapsto \sum_{(h)} h_{(1)} \otimes h_{(2)}$;*

(ii) $h \cdot 1 = \varepsilon(h)1$ *for all $h \in H$, where $\varepsilon : H \to K$ is the counit of H;*

(iii) *the K-linear map $\theta : A \otimes_K H \to \mathrm{End}_K(A)$, given by $\theta(a \otimes h)(b) = a(h \cdot b)$, is bijective.*

I. Counting Hopf-Galois Structures

Definition

Let L/K be a finite extension of fields. A **Hopf-Galois structure** *on L/K consists of a K-Hopf algebra H acting on L and making it into an H-Galois extension of K in the sense of Chase and Sweedler (1969), i.e.*

(i) $h \cdot (st) = \sum_{(h)} (h_{(1)} \cdot s)(h_{(2)} \cdot t)$ *for all $h \in H$ and $s, t \in L$, where we write the comultiplication on H as $h \mapsto \sum_{(h)} h_{(1)} \otimes h_{(2)}$;*

(ii) $h \cdot 1 = \varepsilon(h)1$ *for all $h \in H$, where $\varepsilon : H \to K$ is the counit of H;*

(iii) *the K-linear map $\theta : A \otimes_K H \to \mathrm{End}_K(A)$, given by $\theta(a \otimes h)(b) = a(h \cdot b)$, is bijective.*

Example

If L/K is a Galois extension and $\Gamma = \mathrm{Gal}(L/K)$, then the group algebra $H = K[\Gamma]$, with its natural action on L. gives a Hopf-Galois structure on L/K. This is the **classical** *Hopf-Galois structure.*

Hopf-Galois extensions were introduced to study inseparable field extensions, and they arise in algebraic geometry as the algebras representing principal homogenous spaces over a finite group scheme.

Hopf-Galois extensions were introduced to study inseparable field extensions, and they arise in algebraic geometry as the algebras representing principal homogenous spaces over a finite group scheme.

We will be concerned with extensions L/K which are already Galois extensions.

Hopf-Galois extensions were introduced to study inseparable field extensions, and they arise in algebraic geometry as the algebras representing principal homogenous spaces over a finite group scheme.

We will be concerned with extensions L/K which are already Galois extensions.
In that case, we have

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.

Hopf-Galois extensions were introduced to study inseparable field extensions, and they arise in algebraic geometry as the algebras representing principal homogenous spaces over a finite group scheme.

We will be concerned with extensions L/K which are already Galois extensions.
In that case, we have

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.

We say $G \subset \mathrm{Perm}(\Gamma)$ is regular if any two (and hence all three) of the following hold:

Hopf-Galois extensions were introduced to study inseparable field extensions, and they arise in algebraic geometry as the algebras representing principal homogenous spaces over a finite group scheme.

We will be concerned with extensions L/K which are already Galois extensions.
In that case, we have

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.

We say $G \subset \mathrm{Perm}(\Gamma)$ is regular if any two (and hence all three) of the following hold:

- G acts transitively on Γ;

Hopf-Galois extensions were introduced to study inseparable field extensions, and they arise in algebraic geometry as the algebras representing principal homogenous spaces over a finite group scheme.

We will be concerned with extensions L/K which are already Galois extensions.
In that case, we have

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.

We say $G \subset \mathrm{Perm}(\Gamma)$ is regular if any two (and hence all three) of the following hold:

- G acts transitively on Γ;
- the stabiliser of some (any) element of Γ is $\{e_G\}$;

Hopf-Galois extensions were introduced to study inseparable field extensions, and they arise in algebraic geometry as the algebras representing principal homogenous spaces over a finite group scheme.

We will be concerned with extensions L/K which are already Galois extensions.
In that case, we have

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.

We say $G \subset \mathrm{Perm}(\Gamma)$ is regular if any two (and hence all three) of the following hold:

- G acts transitively on Γ;
- the stabiliser of some (any) element of Γ is $\{e_G\}$;
- $|G| = |\Gamma|$.

The Hopf algebra corresponding to G is $H = L[G]^\Gamma$, the fixed points under Γ acting both on L (as field automorphisms) and on G (as conjugation by left translations).

The Hopf algebra corresponding to G is $H = L[G]^\Gamma$, the fixed points under Γ acting both on L (as field automorphisms) and on G (as conjugation by left translations).

The **type** of the Hopf-Galois structure is the isomorphism class of G.

The Hopf algebra corresponding to G is $H = L[G]^\Gamma$, the fixed points under Γ acting both on L (as field automorphisms) and on G (as conjugation by left translations).

The **type** of the Hopf-Galois structure is the isomorphism class of G.

Example

If $\Gamma \cong C_2 \times C_2$ *then* L/K *has one Hopf-Galois structure of type* $C_2 \times C_2$ *(the classical one) and* 3 *of type* C_4*.*

The Hopf algebra corresponding to G is $H = L[G]^{\Gamma}$, the fixed points under Γ acting both on L (as field automorphisms) and on G (as conjugation by left translations).

The **type** of the Hopf-Galois structure is the isomorphism class of G.

Example

If $\Gamma \cong C_2 \times C_2$ then L/K has one Hopf-Galois structure of type $C_2 \times C_2$ (the classical one) and 3 of type C_4.

Changing notation, we start with (abstract) finite groups Γ, G.

The Hopf algebra corresponding to G is $H = L[G]^\Gamma$, the fixed points under Γ acting both on L (as field automorphisms) and on G (as conjugation by left translations).

The **type** of the Hopf-Galois structure is the isomorphism class of G.

Example

If $\Gamma \cong C_2 \times C_2$ then L/K has one Hopf-Galois structure of type $C_2 \times C_2$ (the classical one) and 3 of type C_4.

Changing notation, we start with (abstract) finite groups Γ, G.

Definition

$e(\Gamma, G)$ is the number of Hopf-Galois structures of type G on a Galois extension with Galois group $\cong \Gamma$.

The Hopf algebra corresponding to G is $H = L[G]^\Gamma$, the fixed points under Γ acting both on L (as field automorphisms) and on G (as conjugation by left translations).

The **type** of the Hopf-Galois structure is the isomorphism class of G.

Example

If $\Gamma \cong C_2 \times C_2$ then L/K has one Hopf-Galois structure of type $C_2 \times C_2$ (the classical one) and 3 of type C_4.

Changing notation, we start with (abstract) finite groups Γ, G.

Definition

$e(\Gamma, G)$ is the number of Hopf-Galois structures of type G on a Galois extension with Galois group $\cong \Gamma$.

So $e(\Gamma, G)$ is just the number of regular subgroups in $\mathrm{Perm}(\Gamma)$ which are isomorphic to G and normalised by $\lambda(\Gamma)$.

We can avoid calculating in the large group $\mathrm{Perm}(\Gamma)$ by looking at regular *embeddings* instead of regular *subgroups*.

We can avoid calculating in the large group $\mathrm{Perm}(\Gamma)$ by looking at regular *embeddings* instead of regular *subgroups*.

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 can avoid calculating in the large group $\mathrm{Perm}(\Gamma)$ by looking at regular *embeddings* instead of regular *subgroups*.

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 $\mathrm{Perm}(\Gamma) \to \mathrm{Perm}(G)$. Then the inclusion $\lambda(\Gamma) \to \mathrm{Perm}(\Gamma)$ translates to a regular embedding $\beta : \Gamma \to \mathrm{Perm}(G)$.

We can avoid calculating in the large group $\mathrm{Perm}(\Gamma)$ by looking at regular *embeddings* instead of regular *subgroups*.

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 $\mathrm{Perm}(\Gamma) \to \mathrm{Perm}(G)$. Then the inclusion $\lambda(\Gamma) \to \mathrm{Perm}(\Gamma)$ translates to a regular embedding $\beta : \Gamma \to \mathrm{Perm}(G)$.

We can reverse this process, so we get a bijection between regular embeddings $\alpha : G \hookrightarrow \mathrm{Perm}(\Gamma)$ and regular embeddings $\beta : \Gamma \to \mathrm{Perm}(G)$.

We can avoid calculating in the large group $\mathrm{Perm}(\Gamma)$ by looking at regular *embeddings* instead of regular *subgroups*.

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 $\mathrm{Perm}(\Gamma) \to \mathrm{Perm}(G)$. Then the inclusion $\lambda(\Gamma) \to \mathrm{Perm}(\Gamma)$ translates to a regular embedding $\beta : \Gamma \to \mathrm{Perm}(G)$.

We can reverse this process, so we get a bijection between regular embeddings $\alpha : G \hookrightarrow \mathrm{Perm}(\Gamma)$ and regular embeddings $\beta : \Gamma \to \mathrm{Perm}(G)$.

$$\alpha(G) \text{ is normalised by } \lambda(\Gamma) \quad \Leftrightarrow \quad \lambda(\Gamma) \subset \mathrm{Norm}_{\mathrm{Perm}(\Gamma)}(\alpha(G))$$

We can avoid calculating in the large group $\mathrm{Perm}(\Gamma)$ by looking at regular *embeddings* instead of regular *subgroups*.

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 $\mathrm{Perm}(\Gamma) \to \mathrm{Perm}(G)$. Then the inclusion $\lambda(\Gamma) \to \mathrm{Perm}(\Gamma)$ translates to a regular embedding $\beta : \Gamma \to \mathrm{Perm}(G)$.

We can reverse this process, so we get a bijection between regular embeddings $\alpha : G \hookrightarrow \mathrm{Perm}(\Gamma)$ and regular embeddings $\beta : \Gamma \to \mathrm{Perm}(G)$.

$$\begin{aligned} \alpha(G) \text{ is normalised by } \lambda(\Gamma) \quad &\Leftrightarrow \quad \lambda(\Gamma) \subset \mathrm{Norm}_{\mathrm{Perm}(\Gamma)}(\alpha(G)) \\ &\Leftrightarrow \quad \beta(\Gamma) \subset \mathrm{Norm}_{\mathrm{Perm}(G)}(G) = G \end{aligned}$$

We can avoid calculating in the large group $\mathrm{Perm}(\Gamma)$ by looking at regular *embeddings* instead of regular *subgroups*.

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 $\mathrm{Perm}(\Gamma) \to \mathrm{Perm}(G)$. Then the inclusion $\lambda(\Gamma) \to \mathrm{Perm}(\Gamma)$ translates to a regular embedding $\beta : \Gamma \to \mathrm{Perm}(G)$.

We can reverse this process, so we get a bijection between regular embeddings $\alpha : G \hookrightarrow \mathrm{Perm}(\Gamma)$ and regular embeddings $\beta : \Gamma \to \mathrm{Perm}(G)$.

$$\begin{aligned}
\alpha(G) \text{ is normalised by } \lambda(\Gamma) \quad &\Leftrightarrow \quad \lambda(\Gamma) \subset \mathrm{Norm}_{\mathrm{Perm}(\Gamma)}(\alpha(G)) \\
&\Leftrightarrow \quad \beta(\Gamma) \subset \mathrm{Norm}_{\mathrm{Perm}(G)}(G) = G \\
&\Leftrightarrow \quad \beta(\Gamma) \subset G \rtimes \mathrm{Aut}(G) =: \mathrm{Hol}(G).
\end{aligned}$$

We can avoid calculating in the large group $\mathrm{Perm}(\Gamma)$ by looking at regular *embeddings* instead of regular *subgroups*.

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 $\mathrm{Perm}(\Gamma) \to \mathrm{Perm}(G)$. Then the inclusion $\lambda(\Gamma) \to \mathrm{Perm}(\Gamma)$ translates to a regular embedding $\beta : \Gamma \to \mathrm{Perm}(G)$.

We can reverse this process, so we get a bijection between regular embeddings $\alpha : G \hookrightarrow \mathrm{Perm}(\Gamma)$ and regular embeddings $\beta : \Gamma \to \mathrm{Perm}(G)$.

$$\begin{aligned} \alpha(G) \text{ is normalised by } \lambda(\Gamma) \quad &\Leftrightarrow \quad \lambda(\Gamma) \subset \mathrm{Norm}_{\mathrm{Perm}(\Gamma)}(\alpha(G)) \\ &\Leftrightarrow \quad \beta(\Gamma) \subset \mathrm{Norm}_{\mathrm{Perm}(G)}(G) = G \\ &\Leftrightarrow \quad \beta(\Gamma) \subset G \rtimes \mathrm{Aut}(G) =: \mathrm{Hol}(G). \end{aligned}$$

$\mathrm{Hol}(G)$ is the **holomorph** of G.

The regular *subgroups* in $\mathrm{Perm}(\Gamma)$ isomorphic to G are the $\mathrm{Aut}(G)$-orbits of regular *embeddings* $\alpha : G \to \mathrm{Perm}(\Gamma)$.

The regular *subgroups* in $\mathrm{Perm}(\Gamma)$ isomorphic to G are the $\mathrm{Aut}(G)$-orbits of regular *embeddings* $\alpha : G \to \mathrm{Perm}(\Gamma)$.

Thus

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

The regular *subgroups* in $\mathrm{Perm}(\Gamma)$ isomorphic to G are the $\mathrm{Aut}(G)$-orbits of regular *embeddings* $\alpha : G \to \mathrm{Perm}(\Gamma)$.

Thus

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

The regular *subgroups* in $\mathrm{Perm}(\Gamma)$ isomorphic to G are the $\mathrm{Aut}(G)$-orbits of regular *embeddings* $\alpha : G \to \mathrm{Perm}(\Gamma)$.

Thus

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

The regular *subgroups* in $\mathrm{Perm}(\Gamma)$ isomorphic to G are the $\mathrm{Aut}(G)$-orbits of regular *embeddings* $\alpha : G \to \mathrm{Perm}(\Gamma)$.

Thus

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

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. Counting Skew Braces

Definition

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

II. 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. 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. 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. 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. 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 we have a group homomorphism

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

Thus $(B, *)$ acts on $(B, +)$.

If $(B, +, *)$ is a skew brace, then we have a group homomorphism

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

Thus $(B, *)$ acts on $(B, +)$.

We also have a bijection $i : (B, *) \to (B, +)$ induced by the identity map on B. This satisfies the 1-cocycle identity

$$i(bc) = i(b) + \lambda_b(i(c)).$$

If $(B,+,*)$ is a skew brace, then we have a group homomorphism

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

Thus $(B,*)$ acts on $(B,+)$.

We also have a bijection $i:(B,*)\to(B,+)$ induced by the identity map on B. This satisfies the 1-cocycle identity

$$i(bc)=i(b)+\lambda_b(i(c)).$$

Now $\mathrm{Hol}(B,+)=(B,+)\rtimes \mathrm{Aut}(B,+)$, and

$$(i,\lambda):(B,*)\to(B,+)\rtimes \mathrm{Aut}(B,+)$$

is a homomorphism. Indeed, it is a regular embedding.

If $(B, +, *)$ is a skew brace, then we have a group homomorphism

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

Thus $(B, *)$ acts on $(B, +)$.

We also have a bijection $i : (B, *) \to (B, +)$ induced by the identity map on B. This satisfies the 1-cocycle identity

$$i(bc) = i(b) + \lambda_b(i(c)).$$

Now $\mathrm{Hol}(B, +) = (B, +) \rtimes \mathrm{Aut}(B, +)$, and

$$(i, \lambda) : (B, *) \to (B, +) \rtimes \mathrm{Aut}(B, +)$$

is a homomorphism. Indeed, it is a regular embedding.
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 bijective cocycle $M \to A$ with respect to the corresponding action of M on A.

Thus, given finite groups M, A of the same order, regular embeddings $M \to \mathrm{Hol}(A)$ give rise to left skew braces, and conversely. 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.

Thus, given finite groups M, A of the same order, regular embeddings $M \to \mathrm{Hol}(A)$ give rise to left skew braces, and conversely. 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.

Definition

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

Thus, given finite groups M, A of the same order, regular embeddings $M \to \mathrm{Hol}(A)$ give rise to left skew braces, and conversely. 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.

Definition

Let $b(M, A)$ be the number of left skew braces (up to isomorphism of skew braces) 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 $M \to \mathrm{Hol}(A)$.

Thus, given finite groups M, A of the same order, regular embeddings $M \to \mathrm{Hol}(A)$ give rise to left skew braces, and conversely. 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.

Definition

Let $b(M, A)$ be the number of left skew braces (up to isomorphism of skew braces) 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:

The two problems are closely related (but not equivalent):

Thus, given finite groups M, A of the same order, regular embeddings $M \to \mathrm{Hol}(A)$ give rise to left skew braces, and conversely. 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.

Definition

Let $b(M, A)$ be the number of left skew braces (up to isomorphism of skew braces) 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:

The two problems are closely related (but not equivalent):

(a) finding the number $e(\Gamma, G)$ of Hopf-Galois structures of type G on Galois extension of fields s with Galois group Γ,

Thus, given finite groups M, A of the same order, regular embeddings $M \to \mathrm{Hol}(A)$ give rise to left skew braces, and conversely. 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.

Definition

Let $b(M, A)$ be the number of left skew braces (up to isomorphism of skew braces) 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:

The two problems are closely related (but not equivalent):

(a) finding the number $e(\Gamma, G)$ of Hopf-Galois structures of type G on Galois extension of fields s with Galois group Γ, and

(b) finding the number $b(\Gamma, G)$ of left skew braces (up to isomorphism) with multiplicative group Γ and additive group G.

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

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

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

while

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

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

while

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

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

while

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

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.

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

while

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

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.

Thus there is no simple formula relating $e(\Gamma, G)$ and $b(\Gamma, G)$.

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

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

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

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

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

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

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

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

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

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

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

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

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".

Finer invariants of G are $r_q = \mathrm{ord}_q(k)$ for each prime $q \mid e$.

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".

Finer invariants of G are $r_q = \mathrm{ord}_q(k)$ for each prime $q \mid e$.Then

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

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".

Finer invariants of G are $r_q = \mathrm{ord}_q(k)$ for each prime $q \mid e$.Then

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

In general, d, g, z and the r_q do not determine G up to isomorphism.

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".

Finer invariants of G are $r_q = \mathrm{ord}_q(k)$ for each prime $q \mid e$. Then

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

In general, d, g, z and the r_q do not determine G up to isomorphism.

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	10	3	10	6	3	91	1
G_4	51	2	12	3	2	91	1
G_5	36	1	10	1	6	13	7

$\mathrm{Aut}(G)$ is generated by θ where

$$\theta(\sigma) = \sigma, \qquad \theta(\tau) = \sigma^z \tau,$$

and by ϕ_s for $s \in \mathbb{Z}_e^\times$, where

$$\phi_s(\sigma) = \sigma^s, \qquad \phi_s(\tau) = \tau,$$

$\mathrm{Aut}(G)$ is generated by θ where

$$\theta(\sigma) = \sigma, \qquad \theta(\tau) = \sigma^z \tau,$$

and by ϕ_s for $s \in \mathbb{Z}_e^\times$, where

$$\phi_s(\sigma) = \sigma^s, \qquad \phi_s(\tau) = \tau,$$

Thus

$$\mathrm{Aut}(G) \cong \mathbb{Z}_g \rtimes \mathbb{Z}_e^\times, \qquad |\mathrm{Aut}(G)| = g\varphi(e).$$

$\mathrm{Aut}(G)$ is generated by θ where

$$\theta(\sigma) = \sigma, \qquad \theta(\tau) = \sigma^z \tau,$$

and by ϕ_s for $s \in \mathbb{Z}_e^\times$, where

$$\phi_s(\sigma) = \sigma^s, \qquad \phi_s(\tau) = \tau,$$

Thus

$$\mathrm{Aut}(G) \cong \mathbb{Z}_g \rtimes \mathbb{Z}_e^\times, \qquad |\mathrm{Aut}(G)| = g\varphi(e).$$

Write elements of $\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G)$ as $[x, \alpha]$ with $x \in G$ and $\alpha \in \mathrm{Aut}(G)$. The multiplication in $\mathrm{Hol}(G)$, and the action of $\mathrm{Hol}(G)$ on G, are given by

$$[x\alpha][y, \beta] = [x\alpha(y), \alpha\beta], \qquad [x, \alpha] \cdot y = x\alpha(y).$$

$\mathrm{Aut}(G)$ is generated by θ where

$$\theta(\sigma) = \sigma, \qquad \theta(\tau) = \sigma^z \tau,$$

and by ϕ_s for $s \in \mathbb{Z}_e^\times$, where

$$\phi_s(\sigma) = \sigma^s, \qquad \phi_s(\tau) = \tau,$$

Thus

$$\mathrm{Aut}(G) \cong \mathbb{Z}_g \rtimes \mathbb{Z}_e^\times, \qquad |\mathrm{Aut}(G)| = g\varphi(e).$$

Write elements of $\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G)$ as $[x, \alpha]$ with $x \in G$ and $\alpha \in \mathrm{Aut}(G)$. The multiplication in $\mathrm{Hol}(G)$, and the action of $\mathrm{Hol}(G)$ on G, are given by

$$[x\alpha][y, \beta] = [x\alpha(y), \alpha\beta], \qquad [x, \alpha] \cdot y = x\alpha(y).$$

Any element of $\mathrm{Hol}(G)$ can be written $[\sigma^a \tau^b, \theta^c \phi_s]$ for suitable a, b, c, s.

IV. Braces and Hopf-Galois Structures 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. Braces and Hopf-Galois Structures of Squarefree Order

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

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

Let $z = \gcd(e, k-1)$, $g = e/z$ and $\zeta = \gcd(\varepsilon, \kappa - 1)$, $\gamma = \varepsilon/\zeta$.

IV. Braces and Hopf-Galois Structures of Squarefree Order

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

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

Let $z = \gcd(e, k-1)$, $g = e/z$ and $\zeta = \gcd(\varepsilon, \kappa - 1)$, $\gamma = \varepsilon/\zeta$.

Also, let

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

IV. Braces and Hopf-Galois Structures of Squarefree Order

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

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

Let $z = \gcd(e, k-1)$, $g = e/z$ and $\zeta = \gcd(\varepsilon, \kappa - 1)$, $\gamma = \varepsilon/\zeta$.

Also, let

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

The result for skew braces is

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.

IV. Braces and Hopf-Galois Structures of Squarefree Order

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

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

Let $z = \gcd(e, k-1)$, $g = e/z$ and $\zeta = \gcd(\varepsilon, \kappa - 1)$, $\gamma = \varepsilon/\zeta$.

Also, let

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

The result for skew braces is

Theorem 1 (Alabdali + B.)

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

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

The result for Hopf-Galois structures depends in a more complicated way on interplay of the structures of G and Γ.

We can replace κ by any element of

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

without changing the isomorphism type of Γ.

We can replace κ by any element of

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

without changing the isomorphism type of Γ.

The group

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

acts freely $\mathcal{K}$ with $w = \varphi(\gcd(d, \delta))$ orbits.

We can replace κ by any element of

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

without changing the isomorphism type of Γ.

The group

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

acts freely $\mathcal{K}$ with $w = \varphi(\gcd(d, \delta))$ orbits.

Let $\kappa_1, \ldots, \kappa_w$ be a system of orbit representatives.

We can replace κ by any element of

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

without changing the isomorphism type of Γ.

The group

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

acts freely $\mathcal{K}$ with $w = \varphi(\gcd(d, \delta))$ orbits.

Let $\kappa_1, \ldots, \kappa_w$ be a system of orbit representatives.

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

We can replace κ by any element of

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

without changing the isomorphism type of Γ.

The group

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

acts freely $\mathcal{K}$ with $w = \varphi(\gcd(d, \delta))$ orbits.

Let $\kappa_1, \ldots, \kappa_w$ be a system of orbit representatives.

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

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

We can replace κ by any element of

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

without changing the isomorphism type of Γ.

The group

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

acts freely $\mathcal{K}$ with $w = \varphi(\gcd(d, \delta))$ orbits.

Let $\kappa_1, \ldots, \kappa_w$ be a system of orbit representatives.

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

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

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

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

Theorem 2 (Alabdali + B.)

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

Theorem 2 (Alabdali + B.)

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

Remark

Although Theorem 1 is simpler to state than Theorem 2, I do not know how to prove Theorem 1 without proving Theorem 2 first.

Sketch of proofs

$$\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G) = \{[\sigma^a \tau^b, \theta^c \phi_s]\}.$$

Sketch of proofs

$$\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G) = \{[\sigma^a \tau^b, \theta^c \phi_s]\}.$$

Inside $\mathrm{Hol}(G)$, we need to find all regular subgroups isomorphic to Γ.

Sketch of proofs

$$\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G) = \{[\sigma^a\tau^b, \theta^c\phi_s]\}.$$

Inside $\mathrm{Hol}(G)$, we need to find all regular subgroups isomorphic to Γ.

We choose an alternative presentation for Γ:

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

Sketch of proofs

$$\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G) = \{[\sigma^a \tau^b, \theta^c \phi_s]\}.$$

Inside $\mathrm{Hol}(G)$, we need to find all regular subgroups isomorphic to Γ.

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 look for elements $X,\ Y \in \mathrm{Hol}(G)$ satisfying these relations.

Sketch of proofs

$$\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G) = \{[\sigma^a \tau^b, \theta^c \phi_s]\}.$$

Inside $\mathrm{Hol}(G)$, we need to find all regular subgroups isomorphic to Γ.

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 look for elements X, $Y \in \mathrm{Hol}(G)$ satisfying these relations.

As X is in the commutator subgroup of Γ, and so of $\mathrm{Hol}(G)$, it cannot involve τ. It follows that $\gamma \mid e$ if any such subgroups exist.

Sketch of proofs

$$\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G) = \{[\sigma^a \tau^b, \theta^c \phi_s]\}.$$

Inside $\mathrm{Hol}(G)$, we need to find all regular subgroups isomorphic to Γ.

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 look for elements X, $Y \in \mathrm{Hol}(G)$ satisfying these relations.

As X is in the commutator subgroup of Γ, and so of $\mathrm{Hol}(G)$, it cannot involve τ. It follows that $\gamma \mid e$ if any such subgroups exist.

Also, X contains no ϕ_s factor: $X = [\sigma^a, \theta^c]$.

Sketch of proofs

$$\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G) = \{[\sigma^a \tau^b, \theta^c \phi_s]\}.$$

Inside $\mathrm{Hol}(G)$, we need to find all regular subgroups isomorphic to Γ.

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 look for elements X, $Y \in \mathrm{Hol}(G)$ satisfying these relations.

As X is in the commutator subgroup of Γ, and so of $\mathrm{Hol}(G)$, it cannot involve τ. It follows that $\gamma \mid e$ if any such subgroups exist.

Also, X contains no ϕ_s factor: $X = [\sigma^a, \theta^c]$.

We can choose Y of the form $[\sigma^u \tau, \theta^v \phi_t]$ (where τ has exponent 1), at the expense of replacing κ by some κ^r.

Sketch of proofs

$$\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G) = \{[\sigma^a \tau^b, \theta^c \phi_s]\}.$$

Inside $\mathrm{Hol}(G)$, we need to find all regular subgroups isomorphic to Γ.

We choose an alternative presentation for Γ:

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

We look for elements X, $Y \in \mathrm{Hol}(G)$ satisfying these relations.

As X is in the commutator subgroup of Γ, and so of $\mathrm{Hol}(G)$, it cannot involve τ. It follows that $\gamma \mid e$ if any such subgroups exist.

Also, X contains no ϕ_s factor: $X = [\sigma^a, \theta^c]$.

We can choose Y of the form $[\sigma^u \tau, \theta^v \phi_t]$ (where τ has exponent 1), at the expense of replacing κ by some κ^r.

In fact, we can choose Y so $YXY^{-1} = X^{\kappa_h}$ for exactly one $h \in \{1, \ldots, w\}$, so the regular subgroups fall into w families $\mathcal{F}_h$.

Each subgroup in the family $\mathcal{F}_h$ contains exactly $\gamma\varphi(e)w/\varphi(\delta)$ pairs of generators (X, Y) with

$$X = [\sigma^a, \theta^c], \quad Y = [\sigma^u\tau, \theta^v\phi_t], \qquad YXY^{-1} = X^{\kappa_h}.$$

Each subgroup in the family $\mathcal{F}_h$ contains exactly $\gamma\varphi(e)w/\varphi(\delta)$ pairs of generators (X, Y) with

$$X = [\sigma^a, \theta^c], \quad Y = [\sigma^u \tau, \theta^v \phi_t], \qquad YXY^{-1} = X^{\kappa_h}.$$

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 $\mathcal{F}_h$.

Each subgroup in the family $\mathcal{F}_h$ contains exactly $\gamma\varphi(e)w/\varphi(\delta)$ pairs of generators (X, Y) with

$$X = [\sigma^a, \theta^c], \quad Y = [\sigma^u\tau, \theta^v\phi_t], \qquad YXY^{-1} = X^{\kappa_h}.$$

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

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

Each subgroup in the family $\mathcal{F}_h$ contains exactly $\gamma\varphi(e)w/\varphi(\delta)$ pairs of generators (X, Y) with

$$X = [\sigma^a, \theta^c], \quad Y = [\sigma^u \tau, \theta^v \phi_t], \qquad YXY^{-1} = X^{\kappa_h}.$$

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

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

We need to calculate $|\mathcal{N}_h|$.

Each subgroup in the family $\mathcal{F}_h$ contains exactly $\gamma\varphi(e)w/\varphi(\delta)$ pairs of generators (X, Y) with

$$X = [\sigma^a, \theta^c], \quad Y = [\sigma^u\tau, \theta^v\phi_t], \qquad YXY^{-1} = X^{\kappa_h}.$$

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

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

We need to calculate $|\mathcal{N}_h|$.

Let

$$\lambda = z^{-1}(k-1) \in \mathbb{Z}_g^\times, \qquad \mu = k^{-1}\lambda \in \mathbb{Z}_g^\times.$$

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.

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.

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.

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.

Thank you for listening!