Hopf-Galois structures on Galois extensions of degree p^2q and skew braces of order p^2q

Ilaria Del Corso
Università di Pisa

Joint w. w. E. Campedel and A. Caranti

Keele, 2 August 2023

Hopf-Galois structures

Let L/K be finite and separable field extension.

A Hopf-Galois structure (HGS) on L/K is given by a K-Hopf algebra H together with an action $H \curvearrowright L$ giving to L an H-module algebra structure, such that the map

$$\begin{array}{rcl} j : L \otimes H & \longrightarrow & \mathrm{End}_K(L) \\ l \otimes h & \longmapsto & (m \mapsto l h(m)) \end{array} \quad \text{is an isomorphism.}$$

Ex. L/K G-Galois, then $K[G]$ with

$$\Delta : \sigma \to \sigma \otimes \sigma, \quad \varepsilon : \sigma \to 1, \quad \lambda : \sigma \to \sigma^{-1}$$

is a K-Hopf-algebra, L is a $K[G]$-module-algebra, and j is an isomorphism.

$\Longrightarrow$ $K[G]$ gives a HGS on L/K, which is called the *classical structure*.

Hopf-Galois structures

Let L/K be finite and separable field extension.

A Hopf-Galois structure (HGS) on L/K is given by a K-Hopf algebra H together with an action $H \curvearrowright L$ giving to L an H-module algebra structure, such that the map

$$\begin{array}{rcl} j : L \otimes H & \longrightarrow & \mathrm{End}_K(L) \\ l \otimes h & \longmapsto & \big(m \mapsto l h(m)\big) \end{array} \quad \text{is an isomorphism.}$$

Ex. L/K G-Galois, then $K[G]$ with

$$\Delta : \sigma \to \sigma \otimes \sigma, \quad \varepsilon : \sigma \to 1, \quad \lambda : \sigma \to \sigma^{-1}$$

is a K-Hopf-algebra, L is a $K[G]$-module-algebra, and j is an isomorphism.

$\Longrightarrow$ $K[G]$ gives a HGS on L/K, which is called the *classical structure*.

Hopf-Galois structures

Let L/K be finite and separable field extension.

A Hopf-Galois structure (HGS) on L/K is given by a K-Hopf algebra H together with an action $H \curvearrowright L$ giving to L an H-module algebra structure, such that the map

$$\begin{array}{rcl} j : L \otimes H & \longrightarrow & \mathrm{End}_K(L) \\ l \otimes h & \longmapsto & \big(m \mapsto l h(m)\big) \end{array} \quad \text{is an isomorphism.}$$

Ex. L/K G-Galois, then $K[G]$ with

$$\Delta : \sigma \to \sigma \otimes \sigma, \quad \varepsilon : \sigma \to 1, \quad \lambda : \sigma \to \sigma^{-1}$$

is a K-Hopf-algebra, L is a $K[G]$-module-algebra, and j is an isomorphism.

$\Longrightarrow$ $K[G]$ gives a HGS on L/K, which is called the *classical structure*.

Hopf-Galois structures

Let L/K be finite and separable field extension.

A Hopf-Galois structure (HGS) on L/K is given by a K-Hopf algebra H together with an action $H \curvearrowright L$ giving to L an H-module algebra structure, such that the map

$$\begin{array}{rcl} j : L \otimes H & \longrightarrow & \mathrm{End}_K(L) \\ l \otimes h & \longmapsto & \big(m \mapsto l h(m)\big) \end{array} \quad \text{is an isomorphism.}$$

Ex. L/K G-Galois, then $K[G]$ with

$$\Delta : \sigma \to \sigma \otimes \sigma, \quad \varepsilon : \sigma \to 1, \quad \lambda : \sigma \to \sigma^{-1}$$

is a K-Hopf-algebra, L is a $K[G]$-module-algebra, and j is an isomorphism.

$\Longrightarrow$ $K[G]$ gives a HGS on L/K, which is called the *classical structure*.

What are the motivations for studying HG theory?

- A non Galois extension may admit Hopf-Galois structures.
- Any (Hopf-)Galois extension may admit several HG structures.

Why study non classical HGS on Galois extensions?

- Galois-module theory. In the context of number theory, it may be easier to study the structure of the ring of integers with respect to a certain HG structure rather than another (see the work by Byott).

What are the motivations for studying HG theory?

- A non Galois extension may admit Hopf-Galois structures.
- Any (Hopf-)Galois extension may admit several HG structures.

Why study non classical HGS on Galois extensions?

- Galois-module theory. In the context of number theory, it may be easier to study the structure of the ring of integers with respect to a certain HG structure rather than another (see the work by Byott).

What are the motivations for studying HG theory?

- A non Galois extension may admit Hopf-Galois structures.
- Any (Hopf-)Galois extension may admit several HG structures.

Why study non classical HGS on Galois extensions?

- Galois-module theory. In the context of number theory, it may be easier to study the structure of the ring of integers with respect to a certain HG structure rather than another (see the work by Byott).

What are the motivations for studying HG theory?

- A non Galois extension may admit Hopf-Galois structures.
- Any (Hopf-)Galois extension may admit several HG structures.

Why study non classical HGS on Galois extensions?

- Galois-module theory. In the context of number theory, it may be easier to study the structure of the ring of integers with respect to a certain HG structure rather than another (see the work by Byott).

HGS and regular subgroups of the holomorph

$$\{\text{HG structures on the } \Gamma-\text{Galois extension } L/K\} \quad L[G]^{\Gamma}$$
$$\updownarrow \qquad\qquad \updownarrow \qquad [GP87]$$
$$\{\text{regular subgroup of } \mathrm{Perm}(\Gamma) \text{ normalised by } \lambda(\Gamma)\} \quad G$$

- the *type* of the HGS is the isomorphism class of the corresponding regular subgroup.

For each Γ, $G = (G, \cdot)$ finite groups with $|G| = |\Gamma|$, let

- $e(\Gamma, G) = \#$HGS of type G on a Γ-Galois extension
- $e'(\Gamma, G) = \#$regular subgroups of $\mathrm{Hol}(G)$ isomorphic to Γ

$$e(\Gamma, G) = \frac{|\mathrm{Aut}(\Gamma)|}{|\mathrm{Aut}(G)|} e'(\Gamma, G) \qquad [Byo96]$$

HGS and regular subgroups of the holomorph

$$\begin{array}{ccc} \{\text{HG structures on the } \Gamma-\text{Galois extension } L/K\} & L[G]^{\Gamma} & \\ \updownarrow & \updownarrow & [GP87] \\ \{\text{regular subgroup of } \mathrm{Perm}(\Gamma) \text{ normalised by } \lambda(\Gamma)\} & G & \end{array}$$

- the *type* of the HGS is the isomorphism class of the corresponding regular subgroup.

For each Γ, $G = (G, \cdot)$ finite groups with $|G| = |\Gamma|$, let

- $e(\Gamma, G) = \#$HGS of type G on a Γ-Galois extension
- $e'(\Gamma, G) = \#$regular subgroups of $\mathrm{Hol}(G)$ isomorphic to Γ

$$e(\Gamma, G) = \frac{|\mathrm{Aut}(\Gamma)|}{|\mathrm{Aut}(G)|} e'(\Gamma, G) \qquad [Byo96]$$

HGS and regular subgroups of the holomorph

$$\begin{array}{ccc} \{\text{HG structures on the } \Gamma - \text{Galois extension } L/K\} & L[G]^{\Gamma} & \\ \updownarrow & \updownarrow & [GP87] \\ \{\text{regular subgroup of } \mathrm{Perm}(\Gamma) \text{ normalised by } \lambda(\Gamma)\} & G & \end{array}$$

- the *type* of the HGS is the isomorphism class of the corresponding regular subgroup.

For each Γ, $G = (G, \cdot)$ finite groups with $|G| = |\Gamma|$, let

- $e(\Gamma, G) = \#$HGS of type G on a Γ-Galois extension
- $e'(\Gamma, G) = \#$regular subgroups of $\mathrm{Hol}(G)$ isomorphic to Γ

$$e(\Gamma, G) = \frac{|\mathrm{Aut}(\Gamma)|}{|\mathrm{Aut}(G)|} e'(\Gamma, G) \qquad [Byo96]$$

Skew Braces

A *(left) skew brace* is a triple $(G, \cdot, \circ)$ where G is a set and $\cdot$ and $\circ$ are two group operations on G, such that

$$k \circ (gh) = (k \circ g) k^{-1} (k \circ h).$$

$(G, \cdot)$ is called the *additive group* and $(G, \circ)$ the *multiplicative group* of the SB.

The introduction and the study of the skew braces follows that of Rump braces, and was motivated by their relation with the non-degenerate set-theoretic solutions of the Yang-Baxter equation.

Skew Braces

A *(left) skew brace* is a triple $(G, \cdot, \circ)$ where G is a set and $\cdot$ and $\circ$ are two group operations on G, such that

$$k \circ (gh) = (k \circ g)k^{-1}(k \circ h).$$

$(G, \cdot)$ is called the *additive group* and $(G, \circ)$ the *multiplicative group* of the SB.

The introduction and the study of the skew braces follows that of Rump braces, and was motivated by their relation with the non-degenerate set-theoretic solutions of the Yang-Baxter equation.

SB and regular subgroups of the holomorph

Given a group $(G, \cdot)$, by the *(total) number of skew braces on* $(G, \cdot)$ we mean the number of distinct operations "$\circ$" on the set G such that $(G, \cdot, \circ)$ is a skew brace.

- $e''(\Gamma, G) = \#\text{SB } (G, \cdot, \circ)$ such that $(G, \circ) \cong \Gamma$.

$$e''(\Gamma, G) = e'(\Gamma, G) \qquad [GV17]$$

- SB up to isomorphism can be counted in terms of classes of regular subgroups of the holomorph.

SB and regular subgroups of the holomorph

Given a group $(G, \cdot)$, by the *(total) number of skew braces on* $(G, \cdot)$ we mean the number of distinct operations "$\circ$" on the set G such that $(G, \cdot, \circ)$ is a skew brace.

- $e''(\Gamma, G) = \#\mathrm{SB}\ (G, \cdot, \circ)$ such that $(G, \circ) \cong \Gamma$.

$$e''(\Gamma, G) = e'(\Gamma, G) \qquad [GV17]$$

- SB up to isomorphism can be counted in terms of classes of regular subgroups of the holomorph.

SB and regular subgroups of the holomorph

Given a group $(G, \cdot)$, by the *(total) number of skew braces on* $(G, \cdot)$ we mean the number of distinct operations "$\circ$" on the set G such that $(G, \cdot, \circ)$ is a skew brace.

- $e''(\Gamma, G) = \#\mathrm{SB}\ (G, \cdot, \circ)$ such that $(G, \circ) \cong \Gamma$.

$$e''(\Gamma, G) = e'(\Gamma, G) \qquad [GV17]$$

- SB up to isomorphism can be counted in terms of classes of regular subgroups of the holomorph.

The Gamma Functions method

Both the HGS on Galois extensions and the SB relate with regular subgroups of the holomorph of a group G, when G varies in the set of the groups of a fixed cardinality.

Theorem [GV17, CDV18] Let $G = (G, \cdot)$ be a group. TFAE

1. A regular subgroup $N \leq \mathrm{Hol}(G)$
2. A group operation $\circ$ on G s.t. $(G, \cdot, \circ)$ is a *SB*, $(G, \circ) \simeq N$
3. A Gamma Function (GF), namely a map $\gamma : G \to \mathrm{Aut}(G)$ such that

$$\gamma(g\gamma(g)(h)) = \gamma(g)\gamma(h) \qquad \text{(GFE)}$$

γ GF on G $\rightsquigarrow$
– $N = \{ \lambda(g)\gamma(g) : g \in G \}$
– "$\circ$" given by $g \circ h = g\gamma(g)h$

Furthermore, # isomorphism classes of SB $(G, \cdot, \circ)$ = # classes of gamma functions under "conjugation" by elements of $\mathrm{Aut}(G)$: $\gamma^{\alpha}(g) = \alpha\gamma(g^{\alpha^{-1}})\alpha^{-1}$

The Gamma Functions method

Both the HGS on Galois extensions and the SB relate with regular subgroups of the holomorph of a group G, when G varies in the set of the groups of a fixed cardinality.

Theorem [GV17, CDV18] Let $G = (G, \cdot)$ be a group. TFAE

1. A regular subgroup $N \leq \mathrm{Hol}(G)$
2. A group operation $\circ$ on G s.t. $(G, \cdot, \circ)$ is a *SB*, $(G, \circ) \simeq N$
3. A Gamma Function (GF), namely a map $\gamma : G \to \mathrm{Aut}(G)$ such that

$$\gamma(g\gamma(g)(h)) = \gamma(g)\gamma(h) \qquad \text{(GFE)}$$

γ GF on G $\rightsquigarrow$
- $N = \{ \lambda(g)\gamma(g) : g \in G \}$
- "$\circ$" given by $g \circ h = g\gamma(g)h$

Furthermore, # isomorphism classes of SB $(G, \cdot, \circ)$ = # classes of gamma functions under "conjugation" by elements of $\mathrm{Aut}(G)$: $\gamma^{\alpha}(g) = \alpha\gamma(g^{\alpha^{-1}})\alpha^{-1}$

The Gamma Functions method

Both the HGS on Galois extensions and the SB relate with regular subgroups of the holomorph of a group G, when G varies in the set of the groups of a fixed cardinality.

Theorem [GV17, CDV18] Let $G = (G, \cdot)$ be a group. TFAE

1. A regular subgroup $N \leq \mathrm{Hol}(G)$
2. A group operation $\circ$ on G s.t. $(G, \cdot, \circ)$ is a *SB*, $(G, \circ) \simeq N$
3. A Gamma Function (GF), namely a map $\gamma : G \to \mathrm{Aut}(G)$ such that

$$\gamma(g\gamma(g)(h)) = \gamma(g)\gamma(h) \qquad \text{(GFE)}$$

γ GF on G $\rightsquigarrow$
- $N = \{ \lambda(g)\gamma(g) : g \in G \}$
- "$\circ$" given by $g \circ h = g\gamma(g)h$

Furthermore, # isomorphism classes of SB $(G, \cdot, \circ)$ = # classes of gamma functions under "conjugation" by elements of $\mathrm{Aut}(G)$: $\gamma^{\alpha}(g) = \alpha\gamma(g^{\alpha^{-1}})\alpha^{-1}$

The Gamma Functions method

Both the HGS on Galois extensions and the SB relate with regular subgroups of the holomorph of a group G, when G varies in the set of the groups of a fixed cardinality.

Theorem [GV17, CDV18] Let $G = (G, \cdot)$ be a group. TFAE

1. A regular subgroup $N \leq \mathrm{Hol}(G)$
2. A group operation $\circ$ on G s.t. $(G, \cdot, \circ)$ is a *SB*, $(G, \circ) \simeq N$
3. A Gamma Function (GF), namely a map $\gamma : G \to \mathrm{Aut}(G)$ such that

$$\gamma(g\gamma(g)(h)) = \gamma(g)\gamma(h) \qquad \text{(GFE)}$$

γ GF on G $\rightsquigarrow$
- $N = \{ \lambda(g)\gamma(g) : g \in G \}$
- " $\circ$ " given by $g \circ h = g\gamma(g)h$

Furthermore, # isomorphism classes of SB $(G, \cdot, \circ)$ = # classes of gamma functions under "conjugation" by elements of $\mathrm{Aut}(G)$: $\gamma^{\alpha}(g) = \alpha\gamma(g^{\alpha^{-1}})\alpha^{-1}$

The Gamma Functions method

Both the HGS on Galois extensions and the SB relate with regular subgroups of the holomorph of a group G, when G varies in the set of the groups of a fixed cardinality.

Theorem [GV17, CDV18] Let $G = (G, \cdot)$ be a group. TFAE

1. A regular subgroup $N \leq \mathrm{Hol}(G)$
2. A group operation $\circ$ on G s.t. $(G, \cdot, \circ)$ is a *SB*, $(G, \circ) \simeq N$
3. A Gamma Function (GF), namely a map $\gamma : G \to \mathrm{Aut}(G)$ such that

$$\gamma(g\gamma(g)(h)) = \gamma(g)\gamma(h) \qquad \text{(GFE)}$$

γ GF on G $\rightsquigarrow$
- $N = \{ \lambda(g)\gamma(g) : g \in G \}$
- "$\circ$" given by $g \circ h = g\gamma(g)h$

Furthermore, # isomorphism classes of SB $(G, \cdot, \circ)$ = # classes of gamma functions under "conjugation" by elements of $\mathrm{Aut}(G)$: $\gamma^{\alpha}(g) = \alpha\gamma(g^{\alpha^{-1}})\alpha^{-1}$

The Gamma Function method for groups of order p^2q

To count the HGS and the SB of order p^2q with the GF method we need to describe

- all (isomorphism classes of) groups G of order p^2q
- $\mathrm{Aut}(G)$, $\forall G$

Then, for all G, we have to compute all GF on G, namely all functions

$$\gamma\colon G \to \mathrm{Aut}(G), \text{ such that } \gamma(g\gamma_g(h)) = \gamma(g)\gamma(h)$$

Then, for each γ we can determine the group $(G, \circ)$ and its isomorphism class, and therefore the number $e'(\Gamma, G)$, for each Γ, and then compute $e(\Gamma, G)$.

With an additional computational effort, we can compute # isomorphism classes of SB $(G, \cdot, \circ)$:

The Gamma Function method for groups of order p^2q

To count the HGS and the SB of order p^2q with the GF method we need to describe

- all (isomorphism classes of) groups G of order p^2q
- $\mathrm{Aut}(G)$, $\forall G$

Then, for all G, we have to compute all GF on G, namely all functions

$$\gamma \colon G \to \mathrm{Aut}(G), \text{ such that } \gamma(g\gamma_g(h)) = \gamma(g)\gamma(h)$$

Then, for each γ we can determine the group $(G, \circ)$ and its isomorphism class, and therefore the number $e'(\Gamma, G)$, for each Γ, and then compute $e(\Gamma, G)$.

With an additional computational effort, we can compute # isomorphism classes of SB $(G, \cdot, \circ)$:

To count the HGS and the SB of order p^2q with the GF method we need to describe

- all (isomorphism classes of) groups G of order p^2q (Hölder)
- $\mathrm{Aut}(G)$, $\forall G$ [CCDC IJGT21]

Then, for all G, we have to compute all GF on G, namely all functions

$$\gamma\colon G \to \mathrm{Aut}(G), \text{ such that } \gamma(g\gamma_g(h)) = \gamma(g)\gamma(h)$$

Then, for each γ we can determine the group $(G, \circ)$ and its isomorphism class, and therefore the number $e'(\Gamma, G)$, for each Γ, and then compute $e(\Gamma, G)$.

With an additional computational effort, we can compute # isomorphism classes of SB $(G, \cdot, \circ)$:

The Gamma Function method for groups of order p^2q

To count the HGS and the SB of order p^2q with the GF method we need to describe

- all (isomorphism classes of) groups G of order p^2q (Hölder)
- $\mathrm{Aut}(G)$, $\forall G$ [CCDC IJGT21]

Then, for all G, we have to compute all GF on G, namely all functions

$$\gamma\colon G \to \mathrm{Aut}(G), \text{ such that } \gamma(g\gamma_g(h)) = \gamma(g)\gamma(h)$$

Then, for each γ we can determine the group $(G, \circ)$ and its isomorphism class, and therefore the number $e'(\Gamma, G)$, for each Γ, and then compute $e(\Gamma, G)$.

With an additional computational effort, we can compute # isomorphism classes of SB $(G, \cdot, \circ)$:

The Gamma Function method for groups of order p^2q

To count the HGS and the SB of order p^2q with the GF method we need to describe

- all (isomorphism classes of) groups G of order p^2q (Hölder)
- $\mathrm{Aut}(G)$, $\forall G$ [CCDC IJGT21]

Then, for all G, we have to compute all GF on G, namely all functions

$$\gamma\colon G \to \mathrm{Aut}(G), \text{ such that } \gamma(g\gamma_g(h)) = \gamma(g)\gamma(h)$$

Then, for each γ we can determine the group $(G, \circ)$ and its isomorphism class, and therefore the number $e'(\Gamma, G)$, for each Γ, and then compute $e(\Gamma, G)$.

With an additional computational effort, we can compute # isomorphism classes of SB $(G, \cdot, \circ)$:

The Gamma Function method for groups of order p^2q

To count the HGS and the SB of order p^2q with the GF method we need to describe

- all (isomorphism classes of) groups G of order p^2q (Hölder)
- $\mathrm{Aut}(G)$, $\forall G$ [CCDC IJGT21]

Then, for all G, we have to compute all GF on G, namely all functions

$$\gamma \colon G \to \mathrm{Aut}(G), \text{ such that } \gamma(g\gamma_g(h)) = \gamma(g)\gamma(h)$$

Then, for each γ we can determine the group $(G, \circ)$ and its isomorphism class, and therefore the number $e'(\Gamma, G)$, for each Γ, and then compute $e(\Gamma, G)$.

With an additional computational effort, we can compute # isomorphism classes of SB $(G, \cdot, \circ)$:

Groups of order p^2q and their automorphism groups

Type	Conditions	G	$\mathrm{Aut}(G)$
1		$\mathcal{C}_{p^2} \times \mathcal{C}_q$	$\mathcal{C}_{p(p-1)} \times \mathcal{C}_{q-1}$
2	$p \mid q-1$	$\mathcal{C}_q \rtimes_p \mathcal{C}_{p^2}$	$\mathcal{C}_p \times \mathrm{Hol}(\mathcal{C}_q)$
3	$p^2 \mid q-1$	$\mathcal{C}_q \rtimes_1 \mathcal{C}_{p^2}$	$\mathrm{Hol}(\mathcal{C}_q)$
4	$q \mid p-1$	$\mathcal{C}_{p^2} \rtimes \mathcal{C}_q$	$\mathrm{Hol}(\mathcal{C}_{p^2})$
5		$\mathcal{C}_p \times \mathcal{C}_p \times \mathcal{C}_q$	$\mathrm{GL}(2, p) \times \mathcal{C}_{q-1}$
6	$q \mid p-1$	$\mathcal{C}_p \times (\mathcal{C}_p \rtimes \mathcal{C}_q)$	$\mathcal{C}_{p-1} \times \mathrm{Hol}(\mathcal{C}_p)$
7	$q \mid p-1$	$(\mathcal{C}_p \times \mathcal{C}_p) \rtimes_S \mathcal{C}_q$	$\mathrm{Hol}(\mathcal{C}_p \times \mathcal{C}_p)$
8	$3 < q \mid p-1$	$(\mathcal{C}_p \times \mathcal{C}_p) \rtimes_{D0} \mathcal{C}_q$	$\mathrm{Hol}(\mathcal{C}_p) \times \mathrm{Hol}(\mathcal{C}_p)$
9	$2 < q \mid p-1$	$(\mathcal{C}_p \times \mathcal{C}_p) \rtimes_{D1} \mathcal{C}_q$	$(\mathrm{Hol}(\mathcal{C}_p) \times \mathrm{Hol}(\mathcal{C}_p)) \rtimes \mathcal{C}_2$
10	$2 < q \mid p+1$	$(\mathcal{C}_p \times \mathcal{C}_p) \rtimes_C \mathcal{C}_q$	$(\mathcal{C}_p \times \mathcal{C}_p) \rtimes (\mathcal{C}_{p^2-1} \rtimes \mathcal{C}_2)$
11	$p \mid q-1$	$(\mathcal{C}_q \rtimes \mathcal{C}_p) \times \mathcal{C}_p$	$\mathrm{Hol}(\mathcal{C}_p) \times \mathrm{Hol}(\mathcal{C}_q)$

Tool#1: isomorphism of p-Sylow

Theorem (Realizability) Let $(G, \cdot, \circ)$ be a SB of order p^2q, where $p > 2$. Then, $(G, \cdot)$ and $(G, \circ)$ have isomorphic Sylow p-subgroups.

- For any GF on G there is always a Sylow p-subgroup H of G which is $\gamma(H)$-invariant;
- this is equivalent to saying that $(H, \cdot, \circ)$ a subSB of $(G, \cdot, \circ)$

- For our groups [FCC12] $\Rightarrow (H, \cdot) \cong (H, \circ)$

Therefore, if Γ and G are groups of order p^2q $(p > 2)$ with non isomorphic Sylow p-subgroups, then

$$e(\Gamma, G) = e'(\Gamma, G) = 0.$$

As it is well known the same is not true for $p = 2$ (see [Koh07, SV18]).

RQ

Tool#1: isomorphism of p-Sylow

Theorem (Realizability) Let $(G, \cdot, \circ)$ be a SB of order p^2q, where $p > 2$. Then, $(G, \cdot)$ and $(G, \circ)$ have isomorphic Sylow p-subgroups.

- For any GF on G there is always a Sylow p-subgroup H of G which is $\gamma(H)$-invariant;
- this is equivalent to saying that $(H, \cdot, \circ)$ a subSB of $(G, \cdot, \circ)$

- For our groups [FCC12] $\Rightarrow (H, \cdot) \cong (H, \circ)$

Therefore, if Γ and G are groups of order p^2q $(p > 2)$ with non isomorphic Sylow p-subgroups, then

$$e(\Gamma, G) = e'(\Gamma, G) = 0.$$

As it is well known the same is not true for $p = 2$ (see [Koh07, SV18]).

RQ

Tool#1: isomorphism of p-Sylow

Theorem (Realizability) Let $(G, \cdot, \circ)$ be a SB of order p^2q, where $p > 2$. Then, $(G, \cdot)$ and $(G, \circ)$ have isomorphic Sylow p-subgroups.

- For any GF on G there is always a Sylow p-subgroup H of G which is $\gamma(H)$-invariant;
- this is equivalent to saying that $(H, \cdot, \circ)$ a subSB of $(G, \cdot, \circ)$

- For our groups [FCC12] $\Rightarrow (H, \cdot) \cong (H, \circ)$

Therefore, if Γ and G are groups of order p^2q $(p > 2)$ with non isomorphic Sylow p-subgroups, then

$$e(\Gamma, G) = e'(\Gamma, G) = 0.$$

As it is well known the same is not true for $p = 2$ (see [Koh07, SV18]).

RQ

Tool#1: isomorphism of p-Sylow

Theorem (Realizability) Let $(G, \cdot, \circ)$ be a SB of order p^2q, where $p > 2$. Then, $(G, \cdot)$ and $(G, \circ)$ have isomorphic Sylow p-subgroups.

- For any GF on G there is always a Sylow p-subgroup H of G which is $\gamma(H)$-invariant;
- this is equivalent to saying that $(H, \cdot, \circ)$ a subSB of $(G, \cdot, \circ)$

- For our groups [FCC12] $\Rightarrow (H, \cdot) \cong (H, \circ)$

Therefore, if Γ and G are groups of order p^2q $(p > 2)$ with non isomorphic Sylow p-subgroups, then

$$e(\Gamma, G) = e'(\Gamma, G) = 0.$$

As it is well known the same is not true for $p = 2$ (see [Koh07, SV18]).

RQ

Tool#1: isomorphism of p-Sylow

Theorem (Realizability) Let $(G, \cdot, \circ)$ be a SB of order p^2q, where $p > 2$. Then, $(G, \cdot)$ and $(G, \circ)$ have isomorphic Sylow p-subgroups.

- For any GF on G there is always a Sylow p-subgroup H of G which is $\gamma(H)$-invariant;
- this is equivalent to saying that $(H, \cdot, \circ)$ a subSB of $(G, \cdot, \circ)$
- For our groups [FCC12] $\Rightarrow (H, \cdot) \cong (H, \circ)$

Therefore, if Γ and G are groups of order p^2q $(p > 2)$ with non isomorphic Sylow p-subgroups, then

$$e(\Gamma, G) = e'(\Gamma, G) = 0.$$

As it is well known the same is not true for $p = 2$ (see [Koh07, SV18]).

RQ

Tool#1: isomorphism of p-Sylow

Theorem (Realizability) Let $(G, \cdot, \circ)$ be a SB of order p^2q, where $p > 2$. Then, $(G, \cdot)$ and $(G, \circ)$ have isomorphic Sylow p-subgroups.

- For any GF on G there is always a Sylow p-subgroup H of G which is $\gamma(H)$-invariant;
- this is equivalent to saying that $(H, \cdot, \circ)$ a subSB of $(G, \cdot, \circ)$

- For our groups [FCC12] $\Rightarrow (H, \cdot) \cong (H, \circ)$

Therefore, if Γ and G are groups of order p^2q ($p > 2$) with non isomorphic Sylow p-subgroups, then

$$e(\Gamma, G) = e'(\Gamma, G) = 0.$$

As it is well known the same is not true for $p = 2$ (see [Koh07, SV18]).

RQ

Tool#2: homomorphism-like theorem

Let G be a group, $A \leq G$, and $\gamma : A \to \mathrm{Aut}(G)$ a function.
We call γ a *relative gamma function* (RGF) on A if it satisfies the GFE and A is $\gamma(A)$-invariant.

Proposition (Lifting and restriction) G finite, $A, B \leq G$ s.t. $G = AB$.

- Let $\gamma\colon G \to \mathrm{Aut}(G)$ be a GF, such that $B \leq \ker(\gamma)$.
  $\Rightarrow \gamma(ba) = \gamma(a)$
  If A is $\gamma(A)$-invariant, then $\gamma_{|A} : A \to Aut(G)$ is a RGF on A and $\ker(\gamma)$ is invariant under $\tilde{\gamma}(A) := \{\iota(a)\gamma(a) : a \in A\} \leq \mathrm{Aut}(G)$.
- If $\gamma' : A \to \mathrm{Aut}(G)$ is a RGF such that
  1. $\gamma'(A \cap B) \equiv 1$,
  2. B is invariant under $\tilde{\gamma}'(A) := \{\iota(a)\gamma'(a) : a \in A\}$.

  Then $\gamma(ba) = \gamma'(a)$ is a GF on G, and $\ker(\gamma) = \ker(\gamma')B$.

Example: $p \mid q-1$, G of type 1, B q-Sylow. Necessarily $B \leq \ker(\gamma)$; moreover A, the p-Sylow, is characteristic $\Rightarrow \gamma \leftrightarrow \gamma_{|A}$

RQ

Tool#2: homomorphism-like theorem

Let G be a group, $A \leq G$, and $\gamma : A \to \mathrm{Aut}(G)$ a function.
We call γ a *relative gamma function* (RGF) on A if it satisfies the GFE and A is $\gamma(A)$-invariant.

The following Proposition gives a criterion to decide if a GF on G is the extension of a RGF, and conversely to show that a RGF on a subgroup of G can be extended to G.

Proposition (Lifting and restriction) G finite, $A, B \leq G$ s.t. $G = AB$.

- Let $\gamma\colon G \to \mathrm{Aut}(G)$ be a GF, such that $B \leq \ker(\gamma)$.
  $\Rightarrow \gamma(ba) = \gamma(a)$
  If A is $\gamma(A)$-invariant, then $\gamma_{|A} : A \to Aut(G)$ is a RGF on A and $\ker(\gamma)$ is invariant under $\tilde{\gamma}(A) := \{\iota(a)\gamma(a) : a \in A\} \leq \mathrm{Aut}(G)$.
- If $\gamma' : A \to \mathrm{Aut}(G)$ is a RGF such that
  1. $\gamma'(A \cap B) \equiv 1$,
  2. B is invariant under $\tilde{\gamma}'(A) := \{\iota(a)\gamma'(a) : a \in A\}$.

  Then $\gamma(ba) = \gamma'(a)$ is a GF on G, and $\ker(\gamma) = \ker(\gamma')B$.

Example: $p \mid q - 1$, G of type 1, B q-Sylow. Necessarily $B \leq \ker(\gamma)$;

Tool#2: homomorphism-like theorem

Let G be a group, $A \leq G$, and $\gamma : A \to \mathrm{Aut}(G)$ a function.
We call γ a *relative gamma function* (RGF) on A if it satisfies the GFE and A is $\gamma(A)$-invariant.

The following Proposition gives a criterion to decide if a GF on G is the extension of a RGF, and conversely to show that a RGF on a subgroup of G can be extended to G.

Proposition (Lifting and restriction) G finite, $A, B \leq G$ s.t. $G = AB$.

- Let $\gamma\colon G \to \mathrm{Aut}(G)$ be a GF, such that $B \leq \ker(\gamma)$.
  $\Rightarrow \gamma(ba) = \gamma(a)$
  If A is $\gamma(A)$-invariant, then $\gamma_{|A} : A \to Aut(G)$ is a RGF on A and $\ker(\gamma)$ is invariant under $\tilde{\gamma}(A) := \{\iota(a)\gamma(a) : a \in A\} \leq \mathrm{Aut}(G)$.
- If $\gamma' : A \to \mathrm{Aut}(G)$ is a RGF such that
  1. $\gamma'(A \cap B) \equiv 1$,
  2. B is invariant under $\tilde{\gamma}'(A) := \{\iota(a)\gamma'(a) : a \in A\}$.

  Then $\gamma(ba) = \gamma'(a)$ is a GF on G, and $\ker(\gamma) = \ker(\gamma')B$.

Example: $p \mid q-1$, G of type 1, B q-Sylow. Necessarily $B \leq \ker(\gamma)$;

Tool#2: homomorphism-like theorem

Let G be a group, $A \leq G$, and $\gamma : A \to \mathrm{Aut}(G)$ a function.
We call γ a *relative gamma function* (RGF) on A if it satisfies the GFE and A is $\gamma(A)$-invariant.

The following Proposition gives a criterion to decide if a GF on G is the extension of a RGF, and conversely to show that a RGF on a subgroup of G can be extended to G.

Proposition (Lifting and restriction) G finite, $A, B \leq G$ s.t. $G = AB$.

- Let $\gamma\colon G \to \mathrm{Aut}(G)$ be a GF, such that $B \leq \ker(\gamma)$.
  $\Rightarrow \gamma(ba) = \gamma(a)$
  If A is $\gamma(A)$-invariant, then $\gamma_{|A} : A \to Aut(G)$ is a RGF on A and $\ker(\gamma)$ is invariant under $\tilde{\gamma}(A) := \{\iota(a)\gamma(a) : a \in A\} \leq \mathrm{Aut}(G)$.
- If $\gamma' : A \to \mathrm{Aut}(G)$ is a RGF such that
  1. $\gamma'(A \cap B) \equiv 1$,
  2. B is invariant under $\tilde{\gamma}'(A) := \{\iota(a)\gamma'(a) : a \in A\}$.

  Then $\gamma(ba) = \gamma'(a)$ is a GF on G, and $\ker(\gamma) = \ker(\gamma')B$.

Example: $p \mid q-1$, G of type 1, B q-Sylow. Necessarily $B \leq \ker(\gamma)$;

Tool#2: homomorphism-like theorem

Let G be a group, $A \leq G$, and $\gamma : A \to \mathrm{Aut}(G)$ a function.
We call γ a *relative gamma function* (RGF) on A if it satisfies the GFE and A is $\gamma(A)$-invariant.

Proposition (Lifting and restriction) G finite, $A, B \leq G$ s.t. $G = AB$.

- Let $\gamma\colon G \to \mathrm{Aut}(G)$ be a GF, such that $B \leq \ker(\gamma)$.
  $\Rightarrow \gamma(ba) = \gamma(a)$
  If A is $\gamma(A)$-invariant, then $\gamma_{|A} : A \to Aut(G)$ is a RGF on A and $\ker(\gamma)$ is invariant under $\tilde{\gamma}(A) := \{\iota(a)\gamma(a) : a \in A\} \leq \mathrm{Aut}(G)$.
- If $\gamma' : A \to \mathrm{Aut}(G)$ is a RGF such that
  1. $\gamma'(A \cap B) \equiv 1$,
  2. B is invariant under $\tilde{\gamma}'(A) := \{\iota(a)\gamma'(a) : a \in A\}$.

  Then $\gamma(ba) = \gamma'(a)$ is a GF on G, and $\ker(\gamma) = \ker(\gamma')B$.

Example: $p \mid q - 1$, G of type 1, B q-Sylow. Necessarily $B \leq \ker(\gamma)$; moreover A, the p-Sylow, is characteristic $\Rightarrow \gamma \leftrightarrow \gamma_{|A}$

RQ

Tool#3: RGF on cyclic subgroups

Proposition (RGF on cyclic subgroups) G finite group, $A = \langle a \rangle$ a cyclic subgroup of G of order p^n (p odd).

For $\eta \in \mathrm{Aut}(G)$ the following are equivalent.

1. There exists a RGF $\gamma : A \to \mathrm{Aut}(G)$ such that $\gamma(a) = \eta$.
2. - A is η-invariant, and
   - $ord(\eta) \mid p^n$.

Example: $p \mid q-1$, G of type 1, B q-Sylow. Necessarily $B \leq \ker(\gamma)$; moreover A, the p-Sylow, is characteristic $\Rightarrow \gamma \leftrightarrow \gamma_{|A}$;

$$\gamma_{|A} : A \to \mathrm{Aut}(G) = \mathcal{C}_{p(p-1)} \times \mathcal{C}_{q-1}$$

$$|\mathrm{GF}| = |\text{elements of order } \mid p^2 \text{ in } \mathrm{Aut}(G)| = \begin{cases} p^2 \text{ if } p \mid\mid q-1 \\ p^3 \text{ if } p^2 \mid q-1 \end{cases}$$

Tool#3: RGF on cyclic subgroups

Proposition (RGF on cyclic subgroups) G finite group, $A = \langle a \rangle$ a cyclic subgroup of G of order p^n (p odd).

For $\eta \in \mathrm{Aut}(G)$ the following are equivalent.

1. There exists a RGF $\gamma : A \to \mathrm{Aut}(G)$ such that $\gamma(a) = \eta$.
2. - A is η-invariant, and
   - $ord(\eta) \mid p^n$.

Example: $p \mid q-1$, G of type 1, B q-Sylow. Necessarily $B \leq \ker(\gamma)$; moreover A, the p-Sylow, is characteristic $\Rightarrow \gamma \leftrightarrow \gamma_{|A}$;

$$\gamma_{|A} : A \to \mathrm{Aut}(G) = \mathcal{C}_{p(p-1)} \times \mathcal{C}_{q-1}$$

$$|\mathrm{GF}| = |\text{elements of order } \mid p^2 \text{ in } \mathrm{Aut}(G)| = \begin{cases} p^2 \text{ if } p \mid\mid q-1 \\ p^3 \text{ if } p^2 \mid q-1 \end{cases}$$

For $q \nmid p^2 - 1$, the numbers $e'(\Gamma, G)$ are:

$\Gamma \backslash G$	1	2	3
1	p	$2pq$	$2q$
2	$p(p-1)$	$2p(pq-2q+1)$	$2q(p-1)$
3	$p^2(p-1)$	$2p^2q(p-1)$	$2(p^2q-pq-q+1)$

$\Gamma \backslash G$	5	11
5	p^2	$2pq$
11	$p^2(p^2-1)$	$2p(1+qp^2-2q)$

For $q \nmid p^2 - 1$, the numbers $e'(\Gamma, G)$ are:

Γ \ G	1	2	3
1	p	$2pq$	$2q$
2	$p(p-1)$	$2p(pq-2q+1)$	$2q(p-1)$
3	$p^2(p-1)$	$2p^2q(p-1)$	$2(p^2q-pq-q+1)$

Γ \ G	5	11
5	p^2	$2pq$
11	$p^2(p^2-1)$	$2p(1+qp^2-2q)$

Tool#4: duality

Pairing: $\lambda(G)^{inv} = \rho(G)$, where $inv : x \to x^{-1}$,

- the GF associated to the LRR $\lambda(G)$ is $\gamma(x) = 1$, and correspond to the trivial SB $(G, \cdot, \cdot)$
- the GF associated to the RRR $\rho(G)$ is $\gamma(x) = \iota(x^{-1})$: and correspond to the SB $(G, \cdot, \cdot^{opp})$

More generally:

If $N \leq Hol(G)$ is a regular subgroup corresponding to γ then N^{inv} is another regular subgroup of $\mathrm{Hol}(G)$, which corresponds to

$$\widetilde{\gamma}(x) = \iota(x^{-1})\gamma(x^{-1})$$

The two SB $(G, \cdot, \circ)$ and $(G, \cdot, \tilde{\circ})$ are dual to each other (see also [KT20]).

RQ

Tool#4: duality

Pairing: $\lambda(G)^{inv} = \rho(G)$, where $inv : x \to x^{-1}$,

- the GF associated to the LRR $\lambda(G)$ is $\gamma(x) = 1$, and correspond to the trivial SB $(G, \cdot, \cdot)$
- the GF associated to the RRR $\rho(G)$ is $\gamma(x) = \iota(x^{-1})$: and correspond to the SB $(G, \cdot, \cdot^{opp})$

More generally:

If $N \leq Hol(G)$ is a regular subgroup corresponding to γ then N^{inv} is another regular subgroup of $\mathrm{Hol}(G)$, which corresponds to

$$\widetilde{\gamma}(x) = \iota(x^{-1})\gamma(x^{-1})$$

The two SB $(G, \cdot, \circ)$ and $(G, \cdot, \tilde{\circ})$ are dual to each other (see also [KT20]).

RQ

Proposition (Duality)

Let G be a non-abelian group, and $C \leq G$ such that

- C cyclic and characteristic;
- $C \cap Z(G) = \{ 1 \}$;
- additional technical hypothesis.

If γ is a GF on G such that $\gamma(c) = \iota(c^{k_c})$ for every $c \in C$, then

$$\text{either } C \leq \ker(\gamma) \text{ or } C \leq \ker(\widetilde{\gamma}).$$

Therefore, if $\gamma(C) \subseteq Inn(C)$, for all γ, then

$$\begin{aligned} e'(\Gamma, G) &= |\{ \gamma \text{ GF on } G : (G, \circ) \cong \Gamma \}| \\ &= 2 \, |\{ \gamma \text{ GF on } G : (G, \circ) \cong \Gamma \text{ and } C \leq \ker(\gamma) \}| . \end{aligned}$$

RQ p2q

Proposition (Duality)

Let G be a non-abelian group, and $C \leq G$ such that

- C cyclic and characteristic;
- $C \cap Z(G) = \{ 1 \}$;
- additional technical hypothesis.

If γ is a GF on G such that $\gamma(c) = \iota(c^{k_c})$ for every $c \in C$, then

$$\text{either } C \leq \ker(\gamma) \text{ or } C \leq \ker(\widetilde{\gamma}).$$

Therefore, if $\gamma(C) \subseteq Inn(C)$, for all γ, then

$$\begin{aligned} e'(\Gamma, G) &= |\{ \gamma \text{ GF on } G : (G, \circ) \cong \Gamma \}| \\ &= 2\,|\{ \gamma \text{ GF on } G : (G, \circ) \cong \Gamma \text{ and } C \leq \ker(\gamma) \}| \,. \end{aligned}$$

RQ p2q

Example: HGS of degree pq

Let $p > q$ be primes and assume $q \mid p-1$ (the other case is trivial)

Theorem [Byo04] The numbers $e(\Gamma, G)$ of Hopf-Galois structures of type G on a Γ-Galois extension of degree pq is

Γ \ G	$\mathcal{C}_{pq}$	$\mathcal{C}_p \rtimes \mathcal{C}_q$
$\mathcal{C}_{pq}$	1	$2(q-1)$
$\mathcal{C}_p \rtimes \mathcal{C}_q$	p	$2(pq-2p+1)$

To prove this Theorem, we compute with the GF method the number $e'(\Gamma, G)$. Our goal is to find the following table

Γ \ G	$\mathcal{C}_{pq}$	$\mathcal{C}_p \rtimes \mathcal{C}_q$
$\mathcal{C}_{pq}$	1	$2p$
$\mathcal{C}_p \rtimes \mathcal{C}_q$	$q-1$	$2(pq-2p+1)$

from which the previous theorem can be obtained by rescaling.

Example: HGS of degree pq

Let $p > q$ be primes and assume $q \mid p - 1$ (the other case is trivial)

Theorem [Byo04] The numbers $e(\Gamma, G)$ of Hopf-Galois structures of type G on a Γ-Galois extension of degree pq is

$\Gamma \backslash G$	$\mathcal{C}_{pq}$	$\mathcal{C}_p \rtimes \mathcal{C}_q$
$\mathcal{C}_{pq}$	1	$2(q-1)$
$\mathcal{C}_p \rtimes \mathcal{C}_q$	p	$2(pq - 2p + 1)$

To prove this Theorem, we compute with the GF method the number $e'(\Gamma, G)$. Our goal is to find the following table

$\Gamma \backslash G$	$\mathcal{C}_{pq}$	$\mathcal{C}_p \rtimes \mathcal{C}_q$
$\mathcal{C}_{pq}$	1	$2p$
$\mathcal{C}_p \rtimes \mathcal{C}_q$	$q-1$	$2(pq - 2p + 1)$

from which the previous theorem can be obtained by rescaling.

Let $B = < b >$ be the Sylow p-subgroup of G and let $\gamma \colon G \to \mathrm{Aut}(G)$ be a GF.

If $\ker(\gamma) = G$, we get the LRR, namely the trivial SB.
So assume $\ker(\gamma) \lneq G$

If $G = \mathcal{C}_{pq}$, then $B \leq \ker(\gamma)$, since in $\mathrm{Aut}(G) \cong \mathcal{C}_{p-1} \times \mathcal{C}_{q-1}$ there are no elements of order p.

If $G = \mathcal{C}_p \rtimes \mathcal{C}_q$, taking $C = B$ in the Proposition duality, we get that one between γ and $\tilde{\gamma}$ has B in the kernel, so we can assume $B \leq \ker(\gamma)$, and then double the result.

So, let $\ker(\gamma) = B$. Then $|\gamma(G)| = q$.

Our "homomorphism" theorem implies that
the GF on G are exactly the extensions of the RGF defined on a q-Sylow.

RQ

Let $B = < b >$ be the Sylow p-subgroup of G and let $\gamma\colon G \to \mathrm{Aut}(G)$ be a GF.

If $\ker(\gamma) = G$, we get the LRR, namely the trivial SB.
So assume $\ker(\gamma) \lneq G$

If $G = \mathcal{C}_{pq}$, then $B \leq \ker(\gamma)$, since in $\mathrm{Aut}(G) \cong \mathcal{C}_{p-1} \times \mathcal{C}_{q-1}$ there are no elements of order p.

If $G = \mathcal{C}_p \rtimes \mathcal{C}_q$, taking $C = B$ in the Proposition duality, we get that one between γ and $\tilde{\gamma}$ has B in the kernel, so we can assume $B \leq \ker(\gamma)$, and then double the result.

So, let $\ker(\gamma) = B$. Then $|\gamma(G)| = q$.

Our "homomorphism" theorem implies that
the GF on G are exactly the extensions of the RGF defined on a q-Sylow.

RQ

Let $B = < b >$ be the Sylow p-subgroup of G and let $\gamma \colon G \to \mathrm{Aut}(G)$ be a GF.

If $\ker(\gamma) = G$, we get the LRR, namely the trivial SB.
So assume $\ker(\gamma) \lneq G$

If $G = \mathcal{C}_{pq}$, then $B \leq \ker(\gamma)$, since in $\mathrm{Aut}(G) \cong \mathcal{C}_{p-1} \times \mathcal{C}_{q-1}$ there are no elements of order p.

If $G = \mathcal{C}_p \rtimes \mathcal{C}_q$, taking $C = B$ in the Proposition duality, we get that one between γ and $\tilde{\gamma}$ has B in the kernel, so we can assume $B \leq \ker(\gamma)$, and then double the result.

So, let $\ker(\gamma) = B$. Then $|\gamma(G)| = q$.

Our "homomorphism" theorem implies that
the GF on G are exactly the extensions of the RGF defined on a q-Sylow.

RQ

Let $B = < b >$ be the Sylow p-subgroup of G and let $\gamma\colon G \to \mathrm{Aut}(G)$ be a GF.

If $\ker(\gamma) = G$, we get the LRR, namely the trivial SB.
So assume $\ker(\gamma) \lneq G$

If $G = \mathcal{C}_{pq}$, then $B \leq \ker(\gamma)$, since in $\mathrm{Aut}(G) \cong \mathcal{C}_{p-1} \times \mathcal{C}_{q-1}$ there are no elements of order p.

If $G = \mathcal{C}_p \rtimes \mathcal{C}_q$, taking $C = B$ in the Proposition duality, we get that one between γ and $\tilde{\gamma}$ has B in the kernel, so we can assume $B \leq \ker(\gamma)$, and then double the result.

So, let $\ker(\gamma) = B$. Then $|\gamma(G)| = q$.

Our "homomorphism" theorem implies that
the GF on G are exactly the extensions of the RGF defined on a q-Sylow.

RQ

By Tool#3, we can define a RGF on a q-Sylow $A =< a >$ of G

$$\gamma\colon A \to \mathrm{Aut}(G)$$
$$a \mapsto \eta$$

where η has order q, provided that A is $\gamma(A)$ invariant ($\eta(A) = A$).

If $G = \mathcal{C}_{pq}$, then A is the unique q-Sylow, so it is characteristic, and

$$\eta\colon \begin{cases} a \to a \\ b \to b^s \end{cases}$$

where $s \in \mathcal{C}_p^*$ has oder q. This gives $q-1$ GF and for each of them

$$a \circ b \circ a^{\ominus 1} \neq b$$

therefore $(G, \circ)$ is non abelian.

RQ

If $G = \mathcal{C}_p \rtimes \mathcal{C}_q$, then - $\mathrm{Aut}(G) \cong \mathcal{C}_p \rtimes \mathcal{C}_{p-1}$

- $\eta = \iota(x)$ for $x \in G$ of order q.

$A = < a >$ is $\gamma(A)$-invariant of and only if $x = a^s$ for $s \in \{1, \dots, q-1\}$. Therefore, for each of the p choices of the q-Sylow there are $q-1$ choices of η, so $p(q-1)$ GF's on $G = \mathcal{C}_p \rtimes \mathcal{C}_q$.

$$a \circ b \circ a^{\ominus 1} = \iota(a)\gamma(a)(b) = \iota(a^{1+s})(b) \begin{cases} = b & \text{if } s = -1 \\ \neq b & \text{if } s \neq -1 \end{cases}$$

Summarizing: for each q-Sylow (p choices) the $q-1$ GF give in 1 case $(G, \circ)$ abelian, and in $q-2$ cases $(G, \circ)$ non abelian.

Recalling that, in this case we have to double the result we get

Γ \ G	$\mathcal{C}_{pq}$	$\mathcal{C}_p \rtimes \mathcal{C}_q$
$\mathcal{C}_{pq}$	1	$2p$
$\mathcal{C}_p \rtimes \mathcal{C}_q$	$q-1$	$2(pq-2p+1)$

RQ

(i) For $q \nmid p-1$:

$\Gamma \backslash G$	1	2	3
1	p	$2p(p-1)$	$2p(p-1)$
2	pq	$2p(pq-2q+1)$	$2pq(p-1)$
3	pq	$2pq(p-1)$	$2(p^2q-pq-q+1)$

$\Gamma \backslash G$	5	11
5	p^2	$2p(p^2-1)$
11	p^2q	$2p(1+qp^2-2q)$

(ii) For $q \nmid p-1$and $q \mid p+1$:

$\Gamma \backslash G$	5	10
5	p^2	$p(p-1)(q-1)$
10	p^2	$2+2p^2(q-3)-p^3+p^4$

(iii) For $q \mid p-1$:

$\Gamma \backslash G$	1	4
1	p	$2p(q-1)$
4	p^2	$2(p^2q-2p^2+1)$

If $q=2$,

$\Gamma \backslash G$	5	6	7
5	p^2	$2p(p+1)$	$p(3p+1)$
6	p^2	$2p(p+1)$	$p(3p+1)$
7	p^2	$2p^2(p+1)$	$2+p(p+1)(2p-1)$

If $q = 3$,

$\Gamma \backslash G$	5	6	7	9
5	p^2	$4p(p+1)$	$2p(3p+1)$	$4p(p+1)$
6	p	$2p(p+3)$	$4p(p+1)$	$p(3p+5)$
7	p^2	$2p^2(p+1)^2$	$2+p^2(2p^2+3p+2)$	$p(p+1)^3$
9	$p^2(2p-1)$	$4p(p^2+1)$	$2(2p^3+3p^2-2p+1)$	$2+2p+p^3(p+3)$

If $q > 3$,

$\Gamma \backslash G$	5	6
5	p^2	$2p(p+1)(q-1)$
6	p	$2p(p+2q-3)$
7	p^2	$2p^2(p+1)(pq-2p+1)$
8, G_2	p^3	$4p(p^2+pq-3p+1)$
8, $G_k \not\simeq G_2$	p^2	$4p(p^2+pq-3p+1)$
9	p^2	$4p(p^2+pq-3p+1)$

$\Gamma \backslash G$	7	9
5	$p(3p+1)(q-1)$	$2p(p+1)(q-1)$
6	$4(p^2+pq-2p)$	$p(4q+3p-7)$
7	$2+p^2(2p^2+pq+2q-4)$	$p(p+1)(p^2(2q-5)+2p+1)$
8, G_2	$2p(p^2q-4p+pq+2)$	$p(p^3+3p^2-14p+4pq-6)$
8, $G_k \not\simeq G_2$	$4p(2p^2-5p+pq+2)$	$p(p^3+5p^2-18p+4pq+8)$
9	$2(4p^3-9p^2+2p^2q+2p+1)$	$2+4p+p^2(p^2+5p+4q-16)$

$\Gamma \backslash G8$	$G \not\simeq G_{\pm 2}$	$G \simeq G_{\pm 2}$, $q > 5$	$G \simeq G_2$, $q = 5$
5	$4p(p+1)(q-1)$	$4p(p+1)(q-1)$	$16p(p+1)$
6	$8p(q+p-2)$	$8p(q+p-2)$	$8p(p+3)$
7	$4p^2(p+1)(pq-3p+2)$	$4p^2(p+1)(pq-3p+2)$	$8p^2(p+1)^2$
8	Table 2	Table 1	$4(1+p+3p^2(p+1))$
9	$8p(2p^2+pq-5p+2))$	$4p(3p^2+2pq-8p+3)$	$16p(2p^3-2p+p+1)$

Table 1: G and Γ of type 8, $G \simeq G_k$ for $k = \pm 2$,

Γ	if $q > 7$:
G_2	$2(1 + 5p + 4p^2q - 17p^2 + 7p^3)$
G_3, $G_{\frac{3}{2}}$	$2(7p + 4p^2q - 18p^2 + 7p^3)$
G_{-2}	$2(1 + 6p + 4p^2q - 19p^2 + 8p^3)$
$G_s \not\simeq G_2, G_3, G_{\frac{3}{2}}, G_{-2}$	$8(2p + p^2q - 5p^2 + 2p^3)$
Γ	if $q = 7$:
G_2	$2(1 + 5p + 11p^2 + 7p^3)$
G_3	$2(1 + 4p + 13p^2 + 6p^3)$

Table 2: G and Γ of type 8, $G \simeq G_k \not\simeq G_{\pm 2}$

Γ	if either k or k^{-1} is a solution of $x^2 - x - 1 = 0$:
G_k, G_{1-k}	$2(1 + 5p + 4p^2q - 17p^2 + 7p^3)$
G_{1+k}	$4(3p + 2p^2q - 8p^2 + 3p^3)$
$G_s \not\simeq G_k, G_{1+k}, G_{1-k}$	$8(2p + p^2q - 5p^2 + 2p^3)$
Γ	if k and k^{-1} are the solutions of $x^2 + x + 1 = 0$:
G_k	$2(1 + 6p + 4p^2q - 19p^2 + 8p^3)$
G_{1-k}, $G_{1-k^{-1}}$	$2(7p + 4p^2q - 18p^2 + 7p^3)$
G_{1+k}	$2(1 + 4p + 4p^2q - 15p^2 + 6p^3)$
$G_s \not\simeq G_k, G_{1+k}, G_{1-k}, G_{1-k^{-1}}$	$8(2p + p^2q - 5p^2 + 2p^3)$
Γ	if k and k^{-1} are the solutions of $x^2 - x + 1 = 0$:
G_{-k}	$2(1 + 6p + 4p^2q - 19p^2 + 8p^3)$
G_{1+k}, $G_{1+k^{-1}}$	$2(7p + 4p^2q - 18p^2 + 7p^3)$
G_{1-k}	$2(1 + 4p + 4p^2q - 15p^2 + 6p^3)$
$G_s \not\simeq G_{-k}, G_{1-k}, G_{1+k}, G_{1+k^{-1}}$	$8(2p + p^2q - 5p^2 + 2p^3)$
Γ	if k and k^{-1} are the solutions of $x^2 + 1 = 0$:
G_k	$4(1 + 2p + 2p^2q - 9p^2 + 4p^3)$
G_{1+k}, G_{1-k}	$4(3p + 2p^2q - 8p^2 + 3p^3)$
$G_s \not\simeq G_k, G_{1+k}, G_{1-k}$	$8(2p + p^2q - 5p^2 + 2p^3)$
Γ	if $k^2 \neq \pm k \pm 1, -1$:
G_k, G_{-k}	$2(1 + 6p + 4p^2q - 19p^2 + 8p^3)$
G_{1+k}, $G_{1+k^{-1}}$, G_{1-k}, $G_{1-k^{-1}}$	$2(7p + 4p^2q - 18p^2 + 7p^3)$
$G_s \not\simeq G_{\pm k}, G_{1\pm k}, G_{1\pm k^{-1}}$	$8(2p + p^2q - 5p^2 + 2p^3)$

Final remarks and a (silly?) question

- **Lifting and restriction.** LR In the literature there are many ways for constructing SB, and our construction of GF give one more way. We made a massive use of this argument and of **duality**. duality
- However, our general results are not enough for getting the classification and we need to use a lot of ad hoc arguments.
- **Isomorphism classes of SB of order** p^2q: we computed them and our results agree with those of Acri and Bonatto.
- **Sylow subgroups.** Sylow In the p^2q case (p odd) the Sylow subgroups of $(G, \cdot)$ and $(G, \circ)$ are isomorphic, but this is not always the case in general.

  In our case, Sylow subgroups have another interesting property: there is always $\gamma(P)$-invariant Sylow p-subgroup P, and a $\gamma(Q)$-invariant Sylow q-subgroup Q (in the language of SB this means that both P and Q are subSB).

  Is this always the case or are there examples of SB for which none of the Sylow p-subgroups of $(G, \cdot)$ is a Sylow p-subgroup of $(G, \circ)$, for some p?

Final remarks and a (silly?) question

- **Lifting and restriction.** LR In the literature there are many ways for constructing SB, and our construction of GF give one more way. We made a massive use of this argument and of **duality**. duality
- However, our general results are not enough for getting the classification and we need to use a lot of ad hoc arguments.
- **Isomorphism classes of SB of order** p^2q: we computed them and our results agree with those of Acri and Bonatto.
- **Sylow subgroups.** Sylow In the p^2q case (p odd) the Sylow subgroups of $(G, \cdot)$ and $(G, \circ)$ are isomorphic, but this is not always the case in general.

  In our case, Sylow subgroups have another interesting property: there is always $\gamma(P)$-invariant Sylow p-subgroup P, and a $\gamma(Q)$-invariant Sylow q-subgroup Q (in the language of SB this means that both P and Q are subSB).

  Is this always the case or are there examples of SB for which none of the Sylow p-subgroups of $(G, \cdot)$ is a Sylow p-subgroup of $(G, \circ)$, for some p?

Final remarks and a (silly?) question

- **Lifting and restriction.** LR In the literature there are many ways for constructing SB, and our construction of GF give one more way. We made a massive use of this argument and of **duality**. duality
- However, our general results are not enough for getting the classification and we need to use a lot of ad hoc arguments.
- **Isomorphism classes of SB of order** p^2q: we computed them and our results agree with those of Acri and Bonatto.
- **Sylow subgroups.** Sylow In the p^2q case (p odd) the Sylow subgroups of $(G,\cdot)$ and $(G,\circ)$ are isomorphic, but this is not always the case in general.

  In our case, Sylow subgroups have another interesting property: there is always $\gamma(P)$-invariant Sylow p-subgroup P, and a $\gamma(Q)$-invariant Sylow q-subgroup Q (in the language of SB this means that both P and Q are subSB).

  Is this always the case or are there examples of SB for which none of the Sylow p-subgroups of $(G,\cdot)$ is a Sylow p-subgroup of $(G,\circ)$, for some p?

Final remarks and a (silly?) question

- **Lifting and restriction.** LR In the literature there are many ways for constructing SB, and our construction of GF give one more way. We made a massive use of this argument and of **duality**. duality
- However, our general results are not enough for getting the classification and we need to use a lot of ad hoc arguments.
- **Isomorphism classes of SB of order** p^2q: we computed them and our results agree with those of Acri and Bonatto.
- **Sylow subgroups.** Sylow In the p^2q case (p odd) the Sylow subgroups of $(G, \cdot)$ and $(G, \circ)$ are isomorphic, but this is not always the case in general.

  In our case, Sylow subgroups have another interesting property: there is always $\gamma(P)$-invariant Sylow p-subgroup P, and a $\gamma(Q)$-invariant Sylow q-subgroup Q (in the language of SB this means that both P and Q are subSB).

  Is this always the case or are there examples of SB for which none of the Sylow p-subgroups of $(G, \cdot)$ is a Sylow p-subgroup of $(G, \circ)$, for some p?

Final remarks and a (silly?) question

- **Lifting and restriction.** LR In the literature there are many ways for constructing SB, and our construction of GF give one more way. We made a massive use of this argument and of **duality**. duality
- However, our general results are not enough for getting the classification and we need to use a lot of ad hoc arguments.
- **Isomorphism classes of SB of order** p^2q: we computed them and our results agree with those of Acri and Bonatto.
- **Sylow subgroups.** Sylow In the p^2q case (p odd) the Sylow subgroups of $(G,\cdot)$ and $(G,\circ)$ are isomorphic, but this is not always the case in general.
  In our case, Sylow subgroups have another interesting property: there is always $\gamma(P)$-invariant Sylow p-subgroup P, and a $\gamma(Q)$-invariant Sylow q-subgroup Q (in the language of SB this means that both P and Q are subSB).
  Is this always the case or are there examples of SB for which none of the Sylow p-subgroups of $(G,\cdot)$ is a Sylow p-subgroup of $(G,\circ)$, for some p?

Thank you!

References i

[AB18] Ali A. Alabdali and Nigel P. Byott, *Counting Hopf-Galois structures on cyclic field extensions of squarefree degree*, J. Algebra **493** (2018), 1–19.

[AB19] Ali A. Alabdali and Nigel P. Byott, *Skew Braces of Squarefree Order*, arXiv e-prints (2019), `https://arxiv.org/abs/1910.07814`.

[Byo96] Nigel P. Byott, *Uniqueness of Hopf Galois structure for separable field extensions*, Comm. Algebra **24** (1996), no. 10, 3217–3228.

[Byo04] Nigel P. Byott, *Hopf-Galois structures on Galois field extensions of degree pq*, J. Pure Appl. Algebra **188** (2004), no. 1-3, 45–57.

[CCDC19] E. Campedel, A. Caranti, and I. Del Corso, *The automorphism groups of the groups of order* p^2q, Int. J. Group Theory **10** (2021), no. 3, 149–157.

[CCDC20] E. Campedel, A. Caranti, and I. Del Corso, *Hopf-Galois structures on extensions of degree p^2q and skew braces of order p^2q: The cyclic Sylow p-subgroup case*, J. Algebra **556** (2020), 1165–1210.

[CCDC22] E. Campedel, A. Caranti, and I. Del Corso, *Hopf-Galois structures on extensions of degree p^2q and skew braces of order p^2q: The elementary abelian Sylow p-subgroup case*, arXiv, submitted

[CDV17] A. Caranti and F. Dalla Volta, *The multiple holomorph of a finitely generated abelian group*, J. Algebra **481** (2017), 327–347.

[CDV18] A. Caranti and F. Dalla Volta, *Groups that have the same holomorph as a finite perfect group*, J. Algebra **507** (2018), 81–102.

[Chi00] Lindsay N. Childs, *Taming wild extensions: Hopf algebras and local Galois module theory*, Mathematical Surveys and Monographs, vol. 80, American Mathematical Society, Providence, RI, 2000.

[Cre21] Teresa Crespo, *Hopf Galois structures on field extensions of degree twice an odd prime square and their associated skew left braces*, J. Algebra **565** (2021), 282-308.

[GP87] Cornelius Greither and Bodo Pareigis, *Hopf Galois theory for separable field extensions*, J. Algebra **106** (1987), no. 1, 239–258.

[GV17] L. Guarnieri and L. Vendramin, *Skew braces and the Yang-Baxter equation*, Math. Comp. **86** (2017), no. 307, 2519–2534.

[KT20] Alan Koch and Paul J. Truman, *Opposite skew left braces and applications*, J. Algebra **546** (2020), 218–235.

[Koh98] Timothy Kohl, *Classification of the Hopf Galois structures on prime power radical extensions*, J. Algebra **207** (1998), no. 2, 525–546.

[Koh07] Timothy Kohl, *Groups of order $4p$, twisted wreath products and Hopf-Galois theory*, J. Algebra **314** (2007), no. 1, 42–74.

[SV18] Agata Smoktunowicz and Leandro Vendramin, *On skew braces (with an appendix by N. Byott and L. Vendramin)*, J. Comb. Algebra **2** (2018), no. 1, 47–86.

[Zen18] Nejabati Zenouz, *On Hopf-Galois Structures and Skew Braces of Order p^3*, PhD thesis, The University of Exeter (2018), `https://ore.exeter.ac.uk/repository/handle/10871/32248`.

[Zen19] Nejabati Zenouz, *Skew braces and Hopf-Galois structures of Heisenberg type*, J. Algebra **524** (2019), 187–225.