Skew Braces with Additive Group Isomorphic to $C_{p^n} \rtimes C_p$ and Corresponding Hopf-Galois Structures

Kayvan Nejabati Zenouz[1]

University of Greenwich

Hopf algebras and Galois module theory Conference
University of Nebraska (at Virtual) Omaha

May 25, 2020

[1] Email: K.NejabatiZenouz@gre.ac.uk website: www.nejabatiz.com

Contents

Overview

First Part: brief preliminaries, notations, literature on

Yang-Baxter Equation

Skew Braces

Hopf-Galois Structures and Connections

Second Part: results of work in progress on

Skew Braces and Hopf-Galois Structures of Type

$$M_\epsilon \stackrel{\text{def}}{=} C_{p^n} \rtimes C_p$$

$\mathrm{Aut}(M_\epsilon)$

Subgroups of M_ϵ and $\mathrm{Aut}(M_\epsilon)$

$\mathrm{Hol}(M_\epsilon)$

Section Contents

The Yang-Baxter Equation

For a vector space V, an element

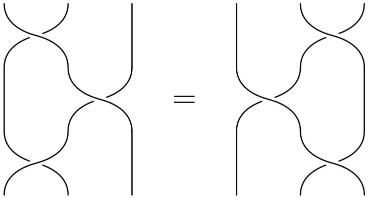
$$R \in \mathrm{GL}(V \otimes V)$$

is said to satisfy the **Yang-Baxter equation (YBE)** if

$$(R \otimes I)(I \otimes R)(R \otimes I) = (I \otimes R)(R \otimes I)(I \otimes R)$$

holds.

This equation can be depicted by



Set-Theoretic Yang-Baxter Equation

In 1992 Drinfeld suggested studying the **simplest class of solutions** arising from the **set-theoretic** version of this equation.

Definition

Let X be a nonempty set and

$$\begin{aligned} r : X \times X &\longrightarrow X \times X \\ (x, y) &\longmapsto (f_x(y), g_y(x)) \end{aligned}$$

a bijection. Then (X, r) is a **set-theoretic solution** of YBE if

$$(r \times \mathrm{id})(\mathrm{id} \times r)(r \times \mathrm{id}) = (\mathrm{id} \times r)(r \times \mathrm{id})(\mathrm{id} \times r)$$

holds. The solution (X, r) is called **non-degenerate** if $f_x, g_x \in \mathrm{Perm}(X)$ for all $x \in X$ and **involutive** if $r^2 = \mathrm{id}$.

Skew Braces

Definition

A (left) **skew brace** is a triple $(B, \oplus, \odot)$ which consists of a set B together with two operations $\oplus$ and $\odot$ so that $(B, \oplus)$ and $(B, \odot)$ are groups such that for all $a, b, c \in B$:

$$a \odot (b \oplus c) = (a \odot b) \ominus a \oplus (a \odot c),$$

where $\ominus a$ is the inverse of a with respect to the operation $\oplus$.

Remark

A skew brace is called **two-sided** if

$$(b \oplus c) \odot a = (b \odot a) \ominus a \oplus (c \odot a),$$

and a **bi-skew brace** if

$$a \oplus (b \odot c) = (a \oplus b) \odot a^{-1} \odot (a \oplus c).$$

Example

Any group $(B, \oplus)$ with

$$a \odot b = a \oplus b \quad \text{(similarly with } a \odot b = b \oplus a\text{)}$$

is a skew brace. This is the **trivial** skew brace structure.

Notation

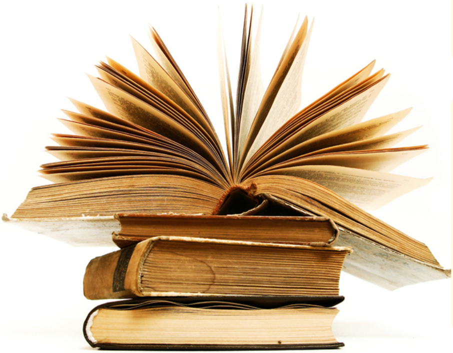
- We call a skew brace $(B, \oplus, \odot)$ such that $(B, \oplus) \cong N$ and $(B, \odot) \cong G$ a G-skew brace of **type** N.
- A skew brace $(B, \oplus, \odot)$ is called a **brace** if $(B, \oplus)$ is abelian, i.e., a skew brace of abelian type.

Braces were introduced by Rump in 2007 as a **generalisation of radical rings**. They provide *non-degenerate, involutive* **set-theoretic solutions of the YBE**.

Skew Braces: History

Skew braces generalise braces and were introduced by Guarnieri and Vendramin in 2017.

They provide *non-degenerate* **set-theoretic solutions of the Yang-Baxter equation**.



Their connection to **ring theory** and **Hopf-Galois structures** was studied by Bachiller, Byott, Smoktunowicz, and Vendramin.

Skew Braces and the YBE

Theorem (Guarnieri and Vendramin)

Let $(B, \oplus, \odot)$ *be a skew brace. Then the map*

$$\begin{aligned} r_B : B \times B &\longrightarrow B \times B \\ (a, b) &\longmapsto \left(\ominus a \oplus (a \odot b), (\ominus a \oplus (a \odot b))^{-1} \odot a \odot b\right) \end{aligned}$$

is a non-degenerate set-theoretic solution of the YBE, which is involutive if and only if $(B, \oplus, \odot)$ *is a brace.*

For L/K extension of fields with $G = \mathrm{Gal}(L/K)$, **Hopf-Galois structures** are K-Hopf algebras together with an action on L.

Definition

A **Hopf-Galois structure** on L/K consists of a finite dimensional cocommutative K-*Hopf algebra* H together with an action on L such that the R-module homomorphism

$$\begin{aligned} j : & L \otimes_K H \longrightarrow \mathrm{End}_K(L) \\ & s \otimes h \longmapsto (t \longmapsto sh(t)) \text{ for } s, t \in L,\ h \in H \end{aligned}$$

is an isomorphism.

The **group algebra** $K[G]$ endows L/K with the classical Hopf-Galois structure.

Theorem (Greither and Pareigis)

Hopf-Galois structures on L/K correspond bijectively to regular subgroups of $\mathrm{Perm}(G)$ *which are normalised by the image of* G*, as left translations, inside* $\mathrm{Perm}(G)$.

Every K-Hopf algebra which endows L/K with a Hopf-Galois structure is of the form $L[N]^G$ for some regular subgroup $N \subseteq \mathrm{Perm}(G)$ normalised by the left translations.

Hopf-Galois Structures: Byott's Translation

Theorem (Byott)

Let G and N be finite groups. There exists a bijection between the sets

$$\mathcal{N} = \{\alpha : N \hookrightarrow \mathrm{Perm}(G) \mid \alpha(N) \text{ is regular and normalised by } G\}$$

$$\mathcal{G} = \{\beta : G \hookrightarrow \mathrm{Hol}(N) \mid \beta(G) \text{ is regular}\},$$

where $\mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N)$.

Enumerating Hopf-Galois Structures (Byott)

Using Byott's translation one can show that

$$\sharp\text{HGS on } L/K \text{ of type } N = \frac{|\mathrm{Aut}\,(G)|}{|\mathrm{Aut}\,(N)|}\,|\{H \subseteq \mathrm{Hol}(N) \text{ regular with } H \cong G\}|\,.$$

Hopf-Galois Structures (HGS): Some Results

- Byott (1996): if $|G| = n$, then L/K has unique HGS iff $\gcd(n, \phi(n)) = 1$
- Kohl (1998, 2019) HGS for C_{p^n}, D_n for a prime $p > 2$
- Byott (1996, 2004) HGS for $|G| = p^2, pq$, also when G a nonabelian simple group
- Carnahan and Childs (1999, 2005) HGS for C_p^n, S_n
- Alabadi and Byott (2017, 2019) HGS for $|G|$ squarefree
- Nejabati Zenouz (2018, 2019) HGS for $|G| = p^3$ where $p \geq 2$
- Crespo and Salguero (2019) HGS for $C_{p^n} \rtimes C_D$ with $p \nmid D$
- Samways (2019) HGS for C_n and Tsang for S_n
- Campedel, Caranti, Del Corso (2019) for $|G| = p^2 q$: the cyclic Sylow p-subgroup case
- Crespo (2020) HGS for $2p^2$, with $p > 2$

Skew Braces Parametrise Hopf-Galois Structures

For a skew brace $(B, \oplus, \odot)$ the group $(B, \oplus)$ acts on $(B, \odot)$ and we find

$$\begin{aligned} d : (B, \oplus) &\longrightarrow \mathrm{Perm}\,(B, \odot) \\ a &\longmapsto (d_a : \; b \longmapsto a \oplus b)\,, \end{aligned}$$

which is a regular embedding.

$$\left\{ \begin{array}{c} \text{isomorphism classes} \\ \text{of } G\text{-skew braces,} \\ \text{i.e., with } (B, \odot) \cong G \end{array} \right\} \overset{\text{bij}}{\leftrightsquigarrow} \left\{ \begin{array}{c} \text{classes of Hopf-Galois structures} \\ \text{on } L/K \text{ under } L[N_1]^G \sim L[N_2]^G \\ \text{if } N_2 = \alpha N_1 \alpha^{-1} \text{ for some} \\ \alpha \in \mathrm{Aut}(G) \end{array} \right\}$$

If $(B, \oplus, \odot)$ is a skew brace of type, then we get the following Hopf-Galois structures on L/K

$$\left\{ L[\alpha\,(\mathrm{Im}\, d)\,\alpha^{-1}]^{(B,\odot)} \mid \alpha \in \mathrm{Aut}\,(B, \odot) \right\}.$$

Automorphism Groups

In particular, if $f : (B, \oplus, \odot) \longrightarrow (B, \oplus, \odot)$ is an automorphism, then we have

$$\begin{array}{ccc} (B, \oplus) & \xhookrightarrow{\ d\ } & \operatorname{Perm}(B, \odot) \\ \wr\Big\downarrow f & & \wr\Big\downarrow C_f \\ (B, \oplus) & \xhookrightarrow{\ d\ } & \operatorname{Perm}(B, \odot)\,; \end{array}$$

using this observation we find

$$\operatorname{Aut}_{\mathcal{B}r}(B, \oplus, \odot) \cong \left\{ \alpha \in \operatorname{Aut}(B, \odot) \mid \alpha\,(\operatorname{Im} d)\,\alpha^{-1} \subseteq \operatorname{Im} d \right\}.$$

Classification of HGS and SB I

Classifying Skew Braces

To find the non-isomorphic G-skew braces of type N classify elements of the set

$$\mathcal{S}(G,N) = \{H \subseteq \mathrm{Perm}\,(G) \mid H \text{ is regular, NLT, } H \cong N\},$$

and extract a maximal subset whose elements are not conjugate by any element of $\mathrm{Aut}\,(G)$.

Hopf-Galois Structures Parametrised by Skew Braces

Denote by B_G^N the isomorphism class of a G-skew brace of type N given by $(B, \oplus, \odot)$. Then the number of Hopf-Galois structures on L/K of type N is given by

$$e(G,N) = \sum_{B_G^N} \frac{|\mathrm{Aut}\,(G)|}{|\mathrm{Aut}_{\mathcal{B}r}\,(B_G^N)|}.$$

Classification of HGS and SB II

We would like to work with **holomorphs** instead of the **permutation groups**.

For a skew brace $(B, \oplus, \odot)$ consider the action of $(B, \odot)$ on $(B, \oplus)$ by $(a, b) \longmapsto a \odot b$. This yeilds to a map

$$\begin{aligned} m : (B, \odot) &\longrightarrow \operatorname{Hol}(B, \oplus) \\ a &\longmapsto (m_a : b \longmapsto a \odot b) \end{aligned}$$

which is a regular embedding. In the above let λ be

$$\begin{array}{ccc} (B, \odot) & \xhookrightarrow{\quad m \quad} & \operatorname{Hol}(B, \oplus) \\ & \searrow^{\lambda} & \downarrow\!\!\downarrow \Theta \\ & & \operatorname{Aut}(B, \oplus) . \end{array}$$

Skew Braces and Regular Subgroups of Holomorph

Bachiller, Byott, Vendramin:

$$\left\{\begin{array}{c}\text{isomorphism classes}\\ \text{of skew braces of}\\ \text{type } N\text{, i.e., with}\\ (B,\oplus)\cong N\end{array}\right\} \overset{\text{bij}}{\leftrightsquigarrow} \left\{\begin{array}{c}\text{classes of regular subgroup of}\\ \mathrm{Hol}(N) \text{ under } H_1\sim H_2 \text{ if}\\ H_2=\alpha H_1\alpha^{-1} \text{ for some}\\ \alpha\in\mathrm{Aut}(N)\end{array}\right\}$$

Another Characterisation of Automorphism Group

$$\mathrm{Aut}_{\mathcal{B}r}\,(B,\oplus,\odot)\cong\left\{\alpha\in\mathrm{Aut}\,(B,\oplus)\mid\alpha\,(\mathrm{Im}\,m)\,\alpha^{-1}\subseteq\mathrm{Im}\,m\right\}$$

Skew braces

To find the non-isomorphic G-skew braces of type N for a fixed N, classify elements of the set

$$\mathcal{S}'(G,N) = \{H \subseteq \mathrm{Hol}\,(N) \mid H \text{ is regular}, \ H \cong G\},$$

and extract a maximal subset whose elements are not conjugate by any element of $\mathrm{Aut}\,(N)$.

Skew Braces: Some Results

- Rump (2007) cyclic braces
- Bachiller (2015) braces of order p^3
- Nejabati Zenouz (2018, 2019) skew braces of order p^3
- Catino, Colazzo, Stefanelli (2017, 2018) semi-braces and skew braces with non-trivial annihilator
- Dietzel (2018) braces of order p^2q
- Childs (2018, 2019) Correspondence and bi-skew braces
- Nasybullov (2018) two-sided skew braces
- Koch, Truman (2019) opposite braces
- Alabadi, Byott (2019) skew braces of squarefree order
- Campedel, Caranti, Del Corso (2019) skew braces of order p^2q: the cyclic Sylow p-subgroup case
- Acri, Bonatto (2019, 2020), skew braces of order pq, p^2q
- Crespo (2019), skew braces of order $2p^2$

Theorem 1 (Nejabati Zenouz, 2018)

Number of G-skew braces of type N, $\widetilde{e}(G,N)$, for $p>3$ prime

$\widetilde{e}(G,N)$	C_{p^3}	$C_{p^2}\times C_p$	C_p^3	$C_p^2\rtimes C_p$	$C_{p^2}\rtimes C_p$
C_{p^3}	3	-	-	-	-
$C_{p^2}\times C_p$	-	9	-	-	$4p+1$
C_p^3	-	-	5	$2p+1$	-
$C_p^2\rtimes C_p$	-	-	$2p+1$	$2p^2-p+3$	-
$C_{p^2}\rtimes C_p$	-	$4p+1$	-	-	$4p^2-3p-1$

Corresponding Hopf-Galois structures $e(G,N)$

$e(G,N)$	C_{p^3}	$C_{p^2}\times C_p$	C_p^3	$C_p^2\rtimes C_p$	$C_{p^2}\rtimes C_p$
C_{p^3}	p^2	-	-	-	-
$C_{p^2}\times C_p$	-	$(2p-1)p^2$	-	-	$(2p-1)(p-1)p^2$
C_p^3	-	-	$(p^4+p^3-1)p^2$	$(p^3-1)(p^2+p-1)p^2$	-
$C_p^2\rtimes C_p$	-	-	$(p^2+p-1)p^2$	$(2p^3-3p+1)p^2$	-
$C_{p^2}\rtimes C_p$	-	$(2p-1)p^2$	-	-	$(2p-1)(p-1)p^2$

Theorem 2 (Nejabati Zenouz, 2018)

Number of G-skew braces of type N, $\widetilde{e}(G,N)$, for $p = 3$ prime

$\widetilde{e}(G,N)$	C_{27}	$C_9 \times C_3$	C_3^3	$C_3^2 \rtimes C_3$	$C_9 \rtimes C_3$
C_{27}	3	-	-	-	-
$C_9 \times C_3$	-	8	1	2	11
C_3^3	-	1	4	5	2
M_1	-	2	5	14	4
M_2	-	11	2	4	22

Corresponding Hopf-Galois structures $e(G,N)$

$e(G,N)$	C_{27}	$C_9 \times C_3$	C_3^3	$C_3^2 \rtimes C_3$	$C_9 \rtimes C_3$
C_{27}	9	-	-	-	-
$C_9 \times C_3$	-	39	6	12	78
C_3^3	-	624	339	1300	1248
M_1	-	48	51	317	96
M_2	-	39	6	12	78

Theorem 3 (Nejabati Zenouz, 2018)

Number of G-skew braces of type N, $\widetilde{e}(G,N)$, for $p=2$ prime

$\widetilde{e}(G,N)$	C_8	$C_4 \times C_2$	C_2^3	D_8	Q_8
C_8	2	-	-	2	2
$C_4 \times C_2$	1	6	3	3	1
C_2^3	-	2	2	1	1
D_8	1	5	2	4	2
Q_8	1	1	1	2	2

Corresponding Hopf-Galois structures $e(G,N)$

$e(G,N)$	C_8	$C_4 \times C_2$	C_2^3	D_8	Q_8
C_8	2	-	-	2	2
$C_4 \times C_2$	4	10	4	6	2
C_2^3	-	42	8	42	14
D_8	2	14	6	6	2
Q_8	6	6	2	6	2

Skew Braces of Semi-direct Product Type

Remark

Note for $p > 3$ we have $p^2 \mid e(G, N)$, and for $p > 2$

$$|\mathrm{Aut}(N)|\, e(G, N) = |\mathrm{Aut}(G)|\, e(N, G) \text{ and } \widetilde{e}(G, N) = \widetilde{e}(N, G).$$

Question

How general is the pattern $\widetilde{e}(G, N) = \widetilde{e}(N, G)$?

Proposition (Nejabati Zenouz, Acri and Bonatto)

Let P and Q be groups. Suppose $\alpha, \beta : Q \longrightarrow \mathrm{Aut}(P)$ are group homomorphisms such that $\mathrm{Im}\,\beta$ is an abelian group and $[\mathrm{Im}\,\alpha, \mathrm{Im}\,\beta] = 1$.

1. We can form an $(P \rtimes_\alpha Q)$-skew brace of type $P \rtimes_\beta Q$.
2. And an $(P \rtimes_\beta Q^{\mathrm{op}})$-skew brace of type $P \rtimes_\alpha Q$.
3. Acri and Bonatto showed that $P \subset \ker \lambda$.

Skew Braces of Type $C_{p^n} \rtimes C_p$ and Corresponding Hopf-Galois Structures

Section Contents

Motivation

- Each column in the tables for Skew braces and Hopf-Galois Structures of Order p^3, except C_{p^3} case, is (was) new.
- *Skew Braces and Hopf-Galois Structures of Heisenberg Type*, J. Algebra, 2019, that is $(B, \oplus)$ is isomorphic to

$$M \overset{\text{def}}{=} \langle \rho, \sigma, \tau \mid \rho^p = \sigma^p = \tau^p = 1,\ \sigma\rho = \rho\sigma,\ \tau\rho = \rho\tau,\ \tau\sigma = \rho\sigma\tau \rangle .$$

- Note, $M \cong C_p^2 \rtimes C_p$. Idea: I could use for $\epsilon = 0, 1$,

$$M_\epsilon \overset{\text{def}}{=} \left\langle \rho, \sigma, \tau \mid \rho^p = \sigma^p = \tau^p = 1,\ \sigma\rho = \rho\sigma,\ \tau\rho = \rho\tau,\ \tau\sigma = \rho^{1-\epsilon}\sigma\tau \right\rangle .$$

- Now $M_0 = M$ and $M_1 = C_p^3$. Then

$$\mathrm{Aut}(M_\epsilon) \subseteq \mathrm{GL}_3(\mathbb{F}_p),$$

and handle both cases at once: too late, too far...

The Group M_ϵ

- Implement the idea for $C_{p^2} \rtimes C_p$ for p prime, so

$$M_\epsilon \stackrel{\text{def}}{=} \left\langle \sigma, \tau \mid \sigma^{p^2} = \tau^p = 1,\ \tau\sigma = \sigma^{p^{\epsilon+1}}\sigma\tau \right\rangle .$$

- Change to $n \geq 2$ with $p > 3$: groups of the form $C_{p^n} \rtimes C_p$.
- Note, a homomorphism

$$\alpha : C_p \longrightarrow \mathrm{Aut}(C_{p^n}) \cong C_{p^{n-1}} \times C_{p-1}$$

is either trivial, or has a unique image of order p.

- Therefore,

$$M_\epsilon \stackrel{\text{def}}{=} \langle \sigma, \tau \mid \sigma^{p^n} = \tau^p = 1,\ \tau\sigma = \sigma^{p^m}\sigma\tau \rangle \cong C_{p^n} \rtimes C_p,$$

where $m = n + \epsilon - 1$, and $m = n$ or $m = n - 1$ only.

- Nonabelian group when $\epsilon = 0$ and abelian when $\epsilon = 1$.

Generalities of M_ϵ

- For positive integers a_1, a_2, a_3, a_4, r we have

$$\sigma^{a_1}\tau^{a_2}\sigma^{a_3}\tau^{a_4} = \sigma^{a_2 a_3 p^m}\sigma^{a_1+a_3}\tau^{a_2+a_4},$$

$$(\sigma^{a_1}\tau^{a_2})^r = \sigma^{\frac{1}{2}a_1 a_2 r(r-1)p^m}\sigma^{a_1 r}\tau^{a_2 r}.$$

- The commutators of two elements $u = \sigma^{u_1}\tau^{u_2}$ and $v = \sigma^{v_1}\tau^{v_2}$ is given by

$$[u, v] = uvu^{-1}v^{-1} = \sigma^{(u_1 v_2 - v_1 u_2)p^m}.$$

Automorphisms of M_ϵ

For $\epsilon = 0, 1$ let

$$\mathrm{L}_\epsilon(\mathbb{F}_p) \stackrel{\text{def}}{=} \left\{ A \in \mathrm{GL}_2(\mathbb{F}_p) \mid A = \begin{pmatrix} a_1 & 0 \\ a_3 & a_4^\epsilon \end{pmatrix} \right\}.$$

Lemma

Every automorphism of $\alpha \in \mathrm{Aut}(M_\epsilon)$ can be written as

$$\alpha = \begin{bmatrix} a_1 & a_2 p^{n-1} \\ a_3 & a_4^\epsilon \end{bmatrix}, \text{ with } \sigma^\alpha = \sigma^{a_1}\tau^{a_3},\ \tau^\alpha = \sigma^{a_2 p^{n-1}}\tau^{a_4^\epsilon},$$

where $a_1 = 0, \ldots, p^n - 1$ and $a_2, a_3, a_4 = 0, \ldots, p - 1$ such that if we reduce the entries modulo p, then we have an element of $\mathrm{L}_\epsilon(\mathbb{F}_p)$. In particular, we have

$$|\mathrm{Aut}(M_\epsilon)| = (p-1)^{\epsilon+1} p^{n+1}.$$

Idea of Proof

- Let $\alpha \in \mathrm{Aut}(M_\epsilon)$. Then we have

$$\sigma^\alpha = \sigma^{a_1}\tau^{a_3}$$
$$\tau^\alpha = \sigma^{a_2}\tau^{a_4}$$

  for some $a_1, a_2, a_3, a_4 \in \mathbb{Z}$.
- Write $\alpha = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}$, first row matters modulo p^n and the second row modulo p.
- Now $\tau^p = 1$ implies $a_2 \equiv 0 \mod p^{n-1}$.
- For α to be injective we need $a_1, a_4 \not\equiv 0 \mod p$.
- We need $(\sigma^\alpha)^{p^m+1}\tau^\alpha = \tau^\alpha\sigma^\alpha$, implies that we need $a_1 a_4 \equiv a_1 \mod p^{n-m}$.
- Thus, $a_4 = 1$ if $m = n-1$ and $a_4 = 1, ..., p-1$ if $m = n$.

Given two automorphisms

$$\alpha = \begin{bmatrix} a_1 & a_2 p^{n-1} \\ a_3 & a_4^{\epsilon} \end{bmatrix} \text{ and } \beta = \begin{bmatrix} b_1 & b_2 p^{n-1} \\ b_3 & b_4^{\epsilon} \end{bmatrix},$$

then the composition $\alpha\beta$ corresponds to

$$\alpha\beta = \begin{bmatrix} a_1 b_1 + a_2 b_3 p^{n-1} + \frac{1}{2} a_1 a_3 b_1 (b_1 - 1) p^m & (a_1 b_2 + a_2 b_4^{\epsilon}) p^{n-1} \\ a_3 b_1 + a_4^{\epsilon} b_3 & (a_4 b_4)^{\epsilon} \end{bmatrix}.$$

Structure of $\mathrm{Aut}(M_\epsilon)$

Lemma

The group $\mathrm{Aut}(M_\epsilon)$ *fits in the exact sequence*

$$1 \longrightarrow C_{p^{n-1}} \times C_p \longrightarrow \mathrm{Aut}(M_\epsilon) \longrightarrow \mathrm{L}_\epsilon(\mathbb{F}_p) \longrightarrow 1.$$

Idea of Proof I

- For $\alpha \in \mathrm{Aut}(M_\epsilon)$ we have $\alpha(\sigma^p) = \sigma^{a_1 p}$.
- Then $Z \overset{\text{def}}{=} \langle \sigma^p \rangle \cong C_{p^{n-1}}$ is a characteristic subgroup of M_ϵ.
- Now α descends on $M_\epsilon / Z \cong C_p^2$, so we have a map

$$\Psi : \mathrm{Aut}(M_\epsilon) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p).$$

- Note that if $\alpha \in \ker \Psi$, then we must have

$$\sigma^\alpha = \sigma^{a_1 p + 1}$$
$$\tau^\alpha = \sigma^{a_2 p^{n-1}} \tau,$$

- This gives

$$\ker \Psi = \left\{ \begin{bmatrix} a_1 p + 1 & a_2 p^{n-1} \\ 0 & 1 \end{bmatrix} \mid a_1 = 0, \ldots, p^{n-1} - 1,\ a_2 = 0, \ldots, p - 1 \right\}.$$

Idea of Proof II

- Take the two automorphisms

$$\beta_1 = \begin{bmatrix} p+1 & 0 \\ 0 & 1 \end{bmatrix}, \ \beta_2 = \begin{bmatrix} 1 & p^{n-1} \\ 0 & 1 \end{bmatrix} \in \ker \Psi.$$

- Note first that $\beta_2^p = 1$ and $\beta_1\beta_2 = \beta_2\beta_1$.
- Use the Lemma that for $p > 3$ and $p \nmid a$ we have

$$(p+1)^{ap^r} = dp^{r+4} + cp^{r+3} + bp^{r+2} + ap^{r+1} + 1,$$

for some integers b, c, d, which gives

$$\beta_1^{p^r}(\sigma) = \sigma^{dp^{r+4}+cp^{r+3}+bp^{r+2}+p^{r+1}+1},$$

- Gives that β_1 has order p^{n-1}, so

$$\ker \Psi = \langle \beta_1, \beta_2 \rangle \cong C_{p^{n-1}} \times C_p.$$

- Follows from earlier Lemma that $\operatorname{Im} \Psi = \mathrm{L}_\epsilon(\mathbb{F}_p)$.

Lemma

The group $\mathrm{Aut}(M_\epsilon)$ *has a unique* p*-Sylow subgroup* $\mathrm{A}(M_\epsilon)$ *isomorphic to*

$$\mathrm{A}(M_\epsilon) = \langle \alpha_1, \alpha_2, \alpha_3 \rangle \cong (C_{p^{n-1}} \times C_p) \rtimes C_p$$

generated by automorphisms

$$\alpha_1 \stackrel{\text{def}}{=} \begin{bmatrix} p+1 & 0 \\ 0 & 1 \end{bmatrix},\ \alpha_2 \stackrel{\text{def}}{=} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},\ \alpha_3 \stackrel{\text{def}}{=} \begin{bmatrix} 1 & p^{n-1} \\ 0 & 1 \end{bmatrix},$$

which satisfy

$$\alpha_1^{p^{n-1}} = \alpha_2^p = \alpha_3^p = 1,$$

$$\alpha_2\alpha_1 = \alpha_1\alpha_2,\ \alpha_3\alpha_1 = \alpha_1\alpha_3,\ \alpha_3\alpha_2 = \alpha_1^{p^{n-2}}\alpha_2\alpha_3.$$

For positive integers a_1, a_2, a_3, a_4, r we have

$$\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\alpha_1^{b_1}\alpha_2^{b_2}\alpha_3^{b_3} = \alpha_1^{a_3 b_2 p^{n-2}}\alpha_1^{a_1+b_1}\alpha_2^{a_2+b_2}\alpha_3^{a_3+b_3},$$

$$(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^r = \alpha_1^{\frac{1}{2}a_2 a_3 r(r-1)p^{n-2}}\alpha_1^{a_1 r}\alpha_2^{a_2 r}\alpha_3^{a_3 r}.$$

Lemma

Let $\alpha \in \mathrm{Aut}(M_\epsilon)$. Then we can always write $\alpha = \alpha_3^{r_3}\beta$, for some r_3 and some $\beta = \begin{bmatrix} b_1 & 0 \\ b_3 & b_4^\epsilon \end{bmatrix} \in \mathrm{Aut}(M_\epsilon)$, and we find

$$\alpha^{-1} = \begin{bmatrix} b_1^{-1} - \frac{1}{2}b_1^{-1}\left(b_1^{-1} - 1\right)b_3 p^m & 0 \\ -b_1^{-1}b_3 b_4^{-\epsilon} & b_4^{-\epsilon} \end{bmatrix}\alpha_3^{-r_3}.$$

In particular, we have

$$\alpha\left(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\right)\alpha^{-1} = \alpha_1^{a_2 r_3 b_1^{-1} b_4^\epsilon p^{n-2} + \frac{1}{2}a_2\left(b_1^{-1}-1\right)p^{m-1} - a_3 b_3 b_4^\epsilon p^{n-2}} \alpha_1^{a_1}\alpha_2^{a_2 b_1^{-1} b_4^\epsilon}\alpha_3^{a_3 b_1 b_4^{-\epsilon}}.$$

Subgroups of M_ϵ up to Automorphisms

Lemma

The strict subgroups of M_ϵ are all abelian and given by the following table (say for $n > 2$).

Order	***Subgroups Up to Automorphisms***
p	$\left\langle \sigma^{p^{n-1}} \right\rangle, \langle \tau \rangle$
p^r	$\left\langle \sigma^{p^{n-r}} \right\rangle, \left\langle \sigma^{p^{n-r}} \tau \right\rangle, \left\langle \sigma^{p^{n-r+1}}, \tau \right\rangle$
p^n	$\langle \sigma \rangle, \langle \sigma^p, \tau \rangle$
p^{n+1}	$\langle \sigma, \tau \rangle$

For $1 < r < n$ *and* $a = 1, ..., p-1$.

Subgroups of $A(M_\epsilon)$

Lemma

Assume n is large. Then subgroups of $\mathrm{A}(M_\epsilon)$ are of the following form

Order	***Subgroups***
p	$\left\langle \alpha_1^{a_1 p^{n-2}} \alpha_2^{a_2} \alpha_3^{a_3} \right\rangle$
p^2	$\left\langle \alpha_1^{a_1 p^{n-3}} \alpha_2^{a_2} \alpha_3^{a_3} \right\rangle, \left\langle \alpha_1^{p^{n-2}}, \alpha_3 \right\rangle, \left\langle \alpha_1^{p^{n-2}}, \alpha_2 \alpha_3^{a_3} \right\rangle$
p^r	$\left\langle \alpha_1^{a_1 p^{n-r-1}} \alpha_2^{a_2} \alpha_3^{a_3} \right\rangle,$ $\left\langle \alpha_1^{p^{n-r}}, \alpha_3 \right\rangle, \left\langle \alpha_1^{p^{n-r}}, \alpha_2 \alpha_3^{a_3} \right\rangle, \left\langle \alpha_1^{a_1 p^{n-r}} \alpha_2, \alpha_1^{a_2 p^{n-r}} \alpha_3 \right\rangle$ $\left\langle \alpha_1^{p^{n-r+1}}, \alpha_2, \alpha_3 \right\rangle$

for some a_1, a_2, a_3, r.

Regular Subgroups of Holomorph

- The holomorph of a group N by

$$\mathrm{Hol}(N) \stackrel{\text{def}}{=} N \rtimes \mathrm{Aut}(N) = \{\eta\alpha \mid \eta \in N,\ \alpha \in \mathrm{Aut}(N)\},$$

  and $\Theta : \mathrm{Hol}(N) \longrightarrow \mathrm{Aut}(N)$ natural projection.
- For $u, v \in N$ and $\alpha, \beta \in \mathrm{Aut}(N)$ write

$$(u\alpha)(v\beta) = uv^{\alpha}\alpha\beta = u(\alpha \cdot v)\alpha\beta.$$

- Regular subgroups H with $|\Theta(H)| = m$ are of the form

$$H = \langle \eta_1, ..., \eta_r, v_1\alpha_1, ..., v_s\alpha_s \rangle,$$

  for some $v_1, ..., v_s \in N$, if such elements exist.
- Let $H_1 = \langle \eta_1, ..., \eta_r \rangle \subseteq N$, and $H_2 = \langle \alpha_1, ..., \alpha_s \rangle \subseteq \mathrm{Aut}(N)$, where $|H_1| = \frac{|H|}{m}$ and $|H_2| = m$.

Generalities of $\mathrm{Hol}(N)$

- We need to check the "*words*" and "*relations*" of

$$H_2 = \langle \alpha_1, ..., \alpha_s \rangle .$$

- For every relation $R(\alpha_1, ..., \alpha_s) = 1$ on H_2, we need

$$R(v_1\alpha_1, ..., v_s\alpha_s) \in H_1$$

  for $|H| = |N|$.
- For every word $W(\alpha_1, ..., \alpha_s) \neq 1$ on H_2, we need

$$W(v_1\alpha_1, ..., v_s\alpha_s)W(\alpha_1, ..., \alpha_s)^{-1} \notin H_1$$

  for H to act freely.

For example, let $r_i = \mathrm{Ord}(\alpha_i)$ and consider regular subgroup

$$H = \langle \eta_1, ..., \eta_r, v_1\alpha_1, ..., v_s\alpha_s \rangle .$$

Then some of the conditions are of the following form

$$\begin{aligned}
(v_i\alpha_i)^{r_i} &= v_i\alpha_i \cdot v_i \cdots \alpha_i^{r_i-1} \cdot v_i\alpha_i^{r_i} \\
&= v_i\alpha_i \cdot v_i \cdots \alpha_i^{r_i-1} \cdot v_i \in H_1 \text{ and} \\
(v_i\alpha_i)^s \alpha^{-s} &= v_i\alpha_i \cdot v_i \cdots \alpha_i^{s-1} \cdot v_i \notin H_1, \text{ for } 0 < s < r_i, \\
(v_i\alpha_i)(\eta_j)(v_i\alpha_i)^{-1} &= v_i(\alpha_i \cdot \eta_j) v_i^{-1} \in H_1 \text{ for all } i, j.
\end{aligned}$$

If H and $\widetilde{H}$ are conjugate by an element of $\beta \in \mathrm{Aut}(N)$, then $\beta(H_1) \subseteq \widetilde{H}_1$ and $\beta H_2 \beta^{-1} \subseteq \widetilde{H}_2$, more precisely,

$$\beta H \beta^{-1} = \left\langle \eta_1^\beta, ..., \eta_r^\beta, v_1^\beta \beta\alpha_1\beta^{-1}, ..., v_s^\beta \beta\alpha_s\beta^{-1} \right\rangle \subseteq \widetilde{H},$$

so can consider subgroups of N up to automorphisms.

Regular Elements of $\mathrm{Hol}(M_\epsilon)$

Regular subgroups of $\mathrm{Hol}(M_\epsilon)$ are contained in

$$M_\epsilon \rtimes A(M_e) = \langle \sigma, \tau, \alpha_1, \alpha_2, \alpha_3 \rangle$$

$$\alpha_1 \stackrel{\mathrm{def}}{=} \begin{bmatrix} p+1 & 0 \\ 0 & 1 \end{bmatrix}, \ \alpha_2 \stackrel{\mathrm{def}}{=} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \ \alpha_3 \stackrel{\mathrm{def}}{=} \begin{bmatrix} 1 & p^{n-1} \\ 0 & 1 \end{bmatrix}.$$

Lemma

Let $g = v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}$ for natural numbers a_1, a_2, a_3, r, and an element $v = \sigma^{v_1}\tau^{v_2} \in M_\epsilon$. Then we have

$$g^r = \sigma^{k_r r p^{n-1} + v_1 \sum_{j=1}^{r-1} (p+1)^{a_1 j} - 1} v^r \tau^{\frac{1}{2} r(r-1) a_2 v_1} \left(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\right)^r$$

for some integer k_r. In particular,

$$g^{p^r} = \sigma^{b_r v_1 p^{r+1} + v_1 p^r} \alpha_1^{a_1 p^r} \text{ for some integer } b_r.$$

Thus if g is regular, its order "depends" on v_1.

Regular Subgroups of $\mathrm{Hol}(M_\epsilon)$

Proposition

Let $G \subset \mathrm{Hol}\,(M_\epsilon)$ be a regular subgroups different from M_ϵ. Let $H_1 = G \cap M_\epsilon = \langle u, v \rangle$ and $H_2 = \Theta(G) \subseteq \mathrm{Aut}(M_\epsilon)$. The following holds.

1. *If $\sigma\tau^d \in H_1$, for some d, then $|\Theta(G)| = p$.*
2. *If $\sigma \notin H_1$, then $\sigma^{p^r} \in H_1$ for some $r < n$.*
3. *If $\tau \in H_1$, then H_2 must have one generator.*
4. *The subgroup G is generated by two elements, and it cannot be outside of the forms*

$$\left\langle \sigma\tau^d, \tau^{w_2}\alpha_1^{a_1 p^{n-2}}\alpha_2^{a_2}\alpha_3^{a_3} \right\rangle, \langle \tau, \sigma^{w_1}\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3} \rangle,$$
$$\langle x\alpha_1^{a_1}, y\alpha_2^{a_2}\alpha_3^{a_3} \rangle, \langle x\alpha_1^{a_1}\alpha_2, y\alpha_1^{a_2}\alpha_3 \rangle.$$

for some $a_1, a_2, a_3, d, w_1, w_2$, and $x, y \in M_\epsilon$.

In order to find the non-isomorphic skew braces we need a general conjugation formula.

Theorem

Let $g = v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}$ *for natural numbers* a_1, a_2, a_3, r, *and an element* $v = \sigma^{v_1}\tau^{v_2} \in M_\epsilon$. *Take* $\alpha = \alpha_3^{r_3}\beta \in \mathrm{Aut}(M_\epsilon)$. *Then we have*

$$\alpha g^r \alpha^{-1} = \sigma^{k_r r p^{n-1} + b_1 v_1 \sum_{j=1}^{r-1} (p+1)^{a_1 j} - 1} (\alpha \cdot v)^r \, \tau^{\frac{1}{2} r(r-1) a_2 b_1 v_1}$$

$$\alpha_1^{a_2 r_3 b_1^{-1} b_4^{\epsilon} r p^{n-2} + a_2 \frac{1}{2}\left(b_1^{-1} - 1\right) r p^{m-1} - a_3 b_3 b_4^{\epsilon} r p^{n-2} + \frac{1}{2} a_2 a_3 r(r-1) p^{n-2}}$$

$$\alpha_1^{a_1 r} \alpha_2^{a_2 b_1^{-1} b_4^{\epsilon} r} \alpha_3^{a_3 b_1 b_4^{-\epsilon} r}$$

for some integer k_r.

Now using the Proposition and Theorem in the previous two slides go through all relevant regular subgroups according to $|\Theta(G)| = p^r$. For each $r = 1, ..., n$:

1. Classify regular subgroups.
2. Find skew braces using conjugation formula.
3. Determine automorphism groups of skew braces.
4. Count Hopf-Galois structures as parametrised by skew braces.

Example $|\Theta(G)| = p$

Proposition

For $|\Theta(G)| = p$ there are exactly $5p-7$ M_0-skew braces of M_0 type and 5 M_1-skew braces of M_0 type. Furthermore, we have 5 M_0-skew braces of M_1 type and 3 M_1-skew braces of M_1 type. I.e., Write $\widetilde{e}(G,N,p)$, the number of skew braces with $|\Theta(G)| = p$. Then we have

$$\begin{aligned}
\widetilde{e}(M_0, M_0, p) &= 5p-7,\\
\widetilde{e}(M_1, M_0, p) &= 5,\\
\widetilde{e}(M_0, M_1, p) &= 5,\\
\widetilde{e}(M_1, M_1, p) &= 3.
\end{aligned}$$

automorphism groups of M_0-skew braces of M_0 type

$$\mathrm{Aut}_{\mathcal{B}r}\left(\left\langle \tau, \sigma\alpha_1^{p^{n-2}} \right\rangle\right) = \left\{ \alpha_3^{r_3} \begin{bmatrix} b_1 & 0 \\ b_3 & 1 \end{bmatrix} \in \mathrm{Aut}(M_0) \mid b_1 \equiv 1 \mod p \right\}$$

$$\mathrm{Aut}_{\mathcal{B}r}\left(\langle \tau, \sigma\alpha_3^{a_3} \rangle\right) = \left\{ \alpha_3^{r_3} \begin{bmatrix} b_1 & 0 \\ b_3 & 1 \end{bmatrix} \in \mathrm{Aut}(M_0) \mid b_3 = 0 \right\} \text{ for } a_3 \neq 0, 1$$

$$\mathrm{Aut}_{\mathcal{B}r}\left(\langle \tau, \sigma\alpha_2^{t}\alpha_3^{a_3} \rangle\right) = \left\{ \alpha_3^{\tilde{r}} \begin{bmatrix} b_1 & 0 \\ b_3 & 1 \end{bmatrix} \in \mathrm{Aut}(M_0) \mid b_1 \equiv \pm 1 \mod p \right\} \text{ for } a_3 \neq 1,\ t = 1, \delta$$

$$\mathrm{Aut}_{\mathcal{B}r}\left(\left\langle \sigma, \tau\alpha_1^{a_1 p^{n-2}} \right\rangle\right) = \left\{ \alpha_3^{r_3} \begin{bmatrix} b_1 & 0 \\ b_3 & 1 \end{bmatrix} \in \mathrm{Aut}(M_0) \mid b_3 = 0 \right\} \text{ for } a_1 \neq -1, 0$$

$$\mathrm{Aut}_{\mathcal{B}r}\left(\left\langle \sigma, \tau\alpha_1^{a_1 p^{n-2}}\alpha_3 \right\rangle\right) = \left\{ \alpha_3^{r_3} \begin{bmatrix} b_1 & 0 \\ b_3 & 1 \end{bmatrix} \in \mathrm{Aut}(M_0) \mid b_3 = 0,\ b_1 = 1 \mod p \right\} \text{ for } a_1 \neq -1$$

automorphism groups M_1-skew braces of M_0 type

$$\mathrm{Aut}_{\mathcal{B}r}\left(\langle \tau, \sigma\alpha_3 \rangle\right) = \left\{ \alpha_3^{r_3} \begin{bmatrix} b_1 & 0 \\ b_3 & 1 \end{bmatrix} \in \mathrm{Aut}(M_0) \mid b_3 = 0 \right\}$$

$$\mathrm{Aut}_{\mathcal{B}r}\left(\langle \tau, \sigma\alpha_2^{t}\alpha_3 \rangle\right) = \left\{ \alpha_3^{\tilde{r}} \begin{bmatrix} b_1 & 0 \\ b_3 & 1 \end{bmatrix} \in \mathrm{Aut}(M_0) \mid b_1 \equiv \pm 1 \mod p \right\} \text{ for } t = 1, \delta$$

$$\mathrm{Aut}_{\mathcal{B}r}\left(\left\langle \sigma, \tau\alpha_1^{-p^{n-2}} \right\rangle\right) = \left\{ \alpha_3^{r_3} \begin{bmatrix} b_1 & 0 \\ b_3 & 1 \end{bmatrix} \in \mathrm{Aut}(M_0) \mid b_3 = 0 \right\}$$

$$\mathrm{Aut}_{\mathcal{B}r}\left(\left\langle \sigma, \tau\alpha_1^{-p^{n-2}}\alpha_3 \right\rangle\right) = \left\{ \alpha_3^{r_3} \begin{bmatrix} b_1 & 0 \\ b_3 & 1 \end{bmatrix} \in \mathrm{Aut}(M_0) \mid b_3 = 0,\ b_1 \equiv 1 \mod p \right\}$$

automorphism groups of M_0-skew braces of M_1 type

$$\mathrm{Aut}_{\mathcal{B}r}\left(\langle \tau, \sigma\alpha_3\rangle\right) = \left\{\alpha_3^{r_3}\begin{bmatrix} b_1 & 0 \\ b_3 & b_4\end{bmatrix} \in \mathrm{Aut}(M_1) \mid b_3 = 0,\ b_4 = 1\right\}$$

$$\mathrm{Aut}_{\mathcal{B}r}\left(\langle \tau, \sigma\alpha_2^t\alpha_3\rangle\right) = \left\{\alpha_3^{\widetilde{r}}\begin{bmatrix} b_1 & 0 \\ b_3 & b_4\end{bmatrix} \in \mathrm{Aut}(M_1) \mid b_1^2 = b_4 \equiv 1 \mod p\right\} \text{ for } t = 1, \delta,$$

$$\mathrm{Aut}_{\mathcal{B}r}\left(\left\langle \sigma, \tau\alpha_1^{p^{n-2}}\right\rangle\right) = \left\{\alpha_3^{r_3}\begin{bmatrix} b_1 & 0 \\ b_3 & b_4\end{bmatrix} \in \mathrm{Aut}(M_1) \mid b_3 = 0,\ b_4 = 1\right\}$$

$$\mathrm{Aut}_{\mathcal{B}r}\left(\left\langle \sigma, \tau\alpha_1^{p^{n-2}}\alpha_3\right\rangle\right) = \left\{\alpha_3^{r_3}\begin{bmatrix} b_1 & 0 \\ b_3 & b_4\end{bmatrix} \in \mathrm{Aut}(M_1) \mid b_3 = 0,\ b_1 = b_4 \equiv 1 \mod p\right\}$$

automorphism groups of M_1-skew braces of M_1 type

$$\mathrm{Aut}_{\mathcal{B}r}\left(\left\langle \tau, \sigma\alpha_1^{p^{n-2}}\right\rangle\right) = \left\{\alpha_3^{r_3}\begin{bmatrix} b_1 & 0 \\ b_3 & b_4\end{bmatrix} \in \mathrm{Aut}(M_1) \mid b_1 \equiv 1 \mod p\right\}$$

$$\mathrm{Aut}_{\mathcal{B}r}\left(\langle \tau, \sigma\alpha_2\rangle\right) = \left\{\alpha_3^{\widetilde{r}}\begin{bmatrix} b_1 & 0 \\ b_3 & b_4\end{bmatrix} \in \mathrm{Aut}(M_1) \mid b_1^2 = b_4 \mod p\right\}$$

$$\mathrm{Aut}_{\mathcal{B}r}\left(\langle \sigma, \tau\alpha_3\rangle\right) = \left\{\alpha_3^{r_3}\begin{bmatrix} b_1 & 0 \\ b_3 & b_4\end{bmatrix} \in \mathrm{Aut}(M_1) \mid b_3 = 0,\ b_1 \equiv b_4^2 \mod p\right\}$$

for some known $\widetilde{r}$.

Corresponding Hopf-Galois Structures

Theorem

Write $e(G,N,p)$, the number of Hopf-Galois structures with $|\Theta(G)| = p$. Then we have

$$\begin{aligned} e(M_0,M_0,p) &= 2p^3-2p^2-p-1, \\ e(M_1,M_0,p) &= 2(p-1)p^2, \\ e(M_0,M_1,p) &= 2p^2, \\ e(M_1,M_1,p) &= (2p+1)(p-1). \end{aligned}$$

Proof.

Follows by using

$$e(G,N,p) = \sum_{B^N_{G,p}} \frac{|\mathrm{Aut}\,(G)|}{\left|\mathrm{Aut}_{\mathcal{B}r}\left(B^N_{G,p}\right)\right|}$$

and $|\mathrm{Aut}(M_\epsilon)| = (p-1)^{\epsilon+1}p^{n+1}$. □

Concluding Remarks

- The case for $r = 2, ..., n$ are work in progress...
- The main ingredient for calculations is encapsulated by the conjugation formula for $\alpha g^r \alpha^{-1}$.
- Remains to check that if $M_\epsilon \hookrightarrow \mathrm{Hol}(G)$ is a regular embedding, for some G, then $G \cong M_0$ or M_1?
- In the above setting G must have at least two generators.
- Ideas can extend to a larger project on metacyclic p-groups.

Thank you for your attention!