Loops of Csörgő Type and the AIM Conjecture

By
Clémence Chanavat

Under the supervision of:
Thibault Gauthier

Master's thesis

École Centrale Lille
Technical University of Prague
Univesité de Lille
August 2021

Contents

Abstract

This thesis proposes to explore the AIM conjecture in loop theory and more particularly loops of Csörgő type, which constituted the first counterexample to the initial version of this conjecture. The AIM conjecture tries to link the abelianess of the group of inner mappings of loops to their nilpotent character. A similar theorem exists in group theory and is proved in an elementary way. Its analog in loop theory remains an open problem and the study of loops of type Csörgő constitutes an interesting angle of attack to advance on this problem. In this thesis, after introducing the necessary theoretical tools, we try to consider computational tracks to generate loops of type Csörgő of size smaller than 128. Their existence to date is an open problem.

Acknowledgements

First, I would like to express my special thanks to Thibault Gauthier and Josef Urban, who supervised and directed me through this entire internship. None of this would have been possible without your advice and your support.

Next, I would like to thanks all the "loop theory" mathematicians and computer scientists community. Understanding their papers and tools, always in open source, was an essential part of my research. Nothing would have been possible without the clarity and accessibility of their work. More particularly, for their precious advice, thank you to David Stanovský, Michael Kinyon, and Petr Vojtěchovský.

I would also like to thank all my CIIRC colleagues whose discussions have been fascinating and inspiring. Finally, a special thanks to Anshula for the support, the motivation, and everything else.

1 Introduction

1.1 Motivations

Group theory began to be developed with the work of Galois and Abel in the 1800s. In addition to becoming an essential branch of mathematics, it has applications in a wide variety of other scientific fields. It can be found in Galois theory, in topology, in geometry, number theory for mathematics but also in physics, chemistry, or cryptography.

Loops are a generalization of groups. The name comes from The Loop, a community area in Chicago, the town where A. A. Albert, a pioneer of non-associative algebra, lived [8]. Loops are very similar to groups, i.e. a set endowed with a multiplication law that satisfies a certain number of axioms. The difference between groups and loops is the lack of associativity of the multiplication law for the loops. Most mathematics is associative and its properties are often used without one even paying attention to it. In loop theory, however, when there are four different ways to interpret $x \cdot y \cdot z \cdot t$, one has to pay attention to the parenthesis, and very quickly, the notations become very cumbersome.

Loops find applications in different fields of mathematics. We can cite the non-null octonions, which have a Moufang loop structure, or the Steiner systems, of which some have a group of automorphisms corresponding to sporadic groups (which appear in the classification of finite groups). Other applications can be found in the theory of code or cryptography, and in the theory of relativity, where the space of velocity vectors has a loop structure.

In the finite case, it is common and practical to represent loops via their multiplication table, or Cayley table. For instance, this is the multiplication table of a loop of order 6 with elements $\{1, 2, 3, 4, 5, 6\}$.

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	3	6	5
3	3	4	5	6	1	2
4	4	3	6	5	2	1
5	5	6	2	1	3	4
6	6	5	1	2	4	3

1.2 The AIM conjecture and Csörgő loops

The AIM conjecture is a loop theory version of an elementary group theory theorem that links the inner automorphisms and the nilpotency class of a group. While the proof in group theory can be done easily, this generalization is still an open problem. More precisely, we define the inner mapping group of a loop, an interesting group constructed as a subspace of the group of bijections from the loop to itself. It generalizes the concept of inner automorphisms in the case of groups. The AIM conjecture is interested in the case where the inner mapping group is abelian. In this case, the conjecture states that the nilpotency class of the loop should be less than three. This conjecture is the direct generalization of a theorem in group theory that states that when the group of inner automorphism is abelian, the group is nilpotent of class less than two.

At first, it was conjectured that the same theorem hold for loops. However, in 2004, Csörgő discovered loops of nilpotency class three with an inner mapping group. Thus the bound of three in the current version of the conjecture. The loop in section 1.1 is an instance of loops with an abelian inner mapping group. Its

nilpotency class is two. The smallest known Csörgő loops have order 128. The goal of this thesis is to generate smaller Csörgő loops.

1.3 Structure of the thesis

In order to find smaller Csörgő loops, we will first describe all the theoretical background necessary to understand the AIM conjecture and the basics of loop theory. Hence, section 2 is dedicated to the basic definitions and properties of loop theory. We will also describe the place of loops and the different structures between the magma and the group. The important notions of nucleus and center are also described in this section. The notation can sometimes be cumbersome, and one should pay attention to the fact that in the left division $y \setminus x$, this is y that is in the denominator.

In the section 3, we will describe the inner mapping group, a central concept in the AIM conjecture. The inner mapping group is a subgroup of the multiplication group. We will also see a very useful theorem that allows us to represent each element of the multiplication group via the product of a translation and an element of the inner mapping group. This will lead to a characterization of the inner mapping group used in the last part of this section. Here, we show that the normal subloops are fully characterized by the inner mapping group.

Now that we have defined the basics of the inner mapping group, we can state the AIM conjecture. This is the content of the section 4. After introducing the nilpotency class of loops, we show how, in the case of group theory, it is related to the inner mapping group. We then explain the AIM conjecture that tries to do the same in the case of loops and explain that the initial version was not successful because of the existence of Csörgő loops. Finally, we describe some type of loops structure where the AIM conjecture was proven true.

The section 5 is dedicated to the construction of Csörgő loops, i.e. loops of nilpotency class three and abelian inner mapping group. This is the most technical section that uses a strategy developed in [5] after the work of Csörgő . To construct Csörgő loops, we use an abelian group H of order 64 with very well chosen properties. We then construct a map μ from a trilinear alternating form that will be used to modify the direct product of H by $\mathbb{Z}_2$. The resulting product will be a Csörgő loop.

Now that we know how to generate Csörgő loops, we will explore in the section 6 the notion of abelian extension. It is an abstract method to generate a new loop from an abelian group and another loop. Those extensions have nice properties, and iterating central extensions leads to all nilpotent loops. In particular, this gives us a way to generate all Csörgő loops theoretically, and hence the smallest ones that we are looking for. We also explicit the construction in section 5 as an iterated central extension.

Finally, in the section 7, we exhibit on small examples interesting structures of the cocycles used in central extension, and we try to exploit them to generate smaller Csörgő loops. After showing that the spaces of search were very vast, we try to reduce it. Hence, we describe a structure of lattice over the cocycles that we exploit through the modification of some groups of order 64 and nilpotency class 3. This method can be a way to generate smaller Csörgő loops.

1.4 Contributions

This thesis proposes to give a rigorous basis and overview of the AIM conjecture and the precise construction of Csörgő loops. Then, we tried to develop a new

method to generate smaller Csörgő loops. Even if it was not successful, with more work, a success might be possible. Indeed, we were able to generate non-associative loops of nilpotency class three and an inner mapping group that is almost abelian (in the sense that its derived group has order 2).

Moreover, tools to compute and generate loops were developed and can be found here `https://github.com/mchana/loopy`. This includes an evaluation algorithm in Python for first-order formulas over finite structures and a Python API to generate and manipulate finite loops. This includes the generation of Csörgő loops described in the paper and, more generally, any abelian extension. Besides, it is possible through this API to communicate and send the loops directly in GAP to do even more computation.

Finally, there are still open problems related to Csörgő loops. Extensions of the work presented here could lead to interesting results. For instance, it is still not known if Csörgő loops of odd order exist. Using iterated central extensions of groups of odd order or modifying groups of odd order and nilpotency class three could lead to a solution. If this method became successful, it could lead to many instances of Csörgő loops and, hopefully, to a wide variety of structures that could provide the mathematical insight needed to prove new results.

2 What is a loop?

In this section, we will describe the basic properties and notations helpful to work with loops. Usually, the concepts we study generalize what we can find in group theory: the center, the commutator, the normal subloop, etc. The goal is often to try to find the best generalizations and to prove the same theorems as in group theory.

2.1 Definitions : magmas, quasigroups and loops

2.1.1 Definitions

The simplest way to define a loop is to take a magma and impose some additional axioms, namely some identity element and existence and unicity of left and right division. More formally:

Definition 1 (Magma)**.** *A magma $(M, \cdot)$ is a set M with a 2-ary law*

$$\cdot : M \times M \mapsto M$$

Definition 2 (Quasigroup)**.** *A quasigroup $(Q, \cdot)$ is a magma where the law satisfies:*

$$\forall (x, y) \in Q \times Q,\ \exists! (r, l) \in Q \times Q,\ x \cdot l = y \wedge r \cdot x = y$$

We note r with $y \,/\, x$ and l with $x \setminus y$, respectively, the right and the left division.

Definition 3 (Loop)**.** *A loop $(L, \cdot, 1)$ is a quasigroup $(Q, \cdot)$ with an additional element $1 \in L$ which satisfies:*

$$\forall x \in L,\ 1 \cdot x = x \cdot 1 = x$$

1 is called the identity element of the loop.

Definition 4 (Group)**.** *A group $(G, \cdot, 1)$ is a loop where the law $\cdot$ satisfies:*

$$\forall (x, y, z) \in Q^3,\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$$

This property is called associativity.

We construct a hierarchy of mathematical structures starting from the magma and ending with the group. Each time, we add one more axiom: cancellation for the magma to the quasigroup, the identity element for the quasigroup to the loop, and associativity for the loop to the group. Starting from the magma and adding axioms in a different order leads to different hierarchies of mathematical structures summarized in the diagram of the figure 1. A more practical definition of a loop uses the left and right translation that can be defined in a magma as follow:

Definition 5 (Translations)**.** *Let $(M, \cdot)$ be a magma and $x \in M$. The left translation L_x is the function*

$$\begin{aligned} L_x \colon M &\to M \\ y &\mapsto x \cdot y \end{aligned}$$

The right translation R_x is the function

$$\begin{aligned} R_x \colon M &\to M \\ y &\mapsto y \cdot x \end{aligned}$$

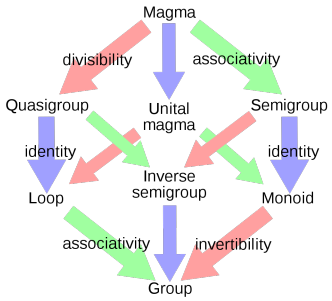

Figure 1: Magma structures and their axioms.
From Wikipedia (Quasigroup)

Then we have

Definition 6 (Loop, alternative definition)**.** *A loop* $(Q, \cdot, 1)$ *is a magma* $(Q, \cdot)$ *where*

- $\forall x \in Q,\ L_x$ *and* R_x *are bijections*
- L_1 *and* R_1 *are identity functions*

We see that the bijective nature of R_x and L_x comes from the unicity of the existence of the right and left divisions, whereas R_1 and L_1 being identities is a rephrasing of the identity axiom. This equivalent definition is sometimes more convenient to do mathematics because we can deal with the composition of functions which is associative. (Note that the associativity of $\cdot$ is, in terms of the right translations, for instance, $\forall (x, y, z) \in L^3,\ R_{xy}R_z = R_xR_{yz}$).
To avoid cumbersome notation, we will avoid using $\cdot$ when we can, and it will have lower precedence than "nothing". That means $xy \cdot z = (x \cdot y) \cdot z$. Similarly, $\backslash$ and $/$ will have stronger precedence than $\cdot$ but a lower than "nothing". That is $xy \backslash z = (xy) \backslash z$ and $xy \cdot z / z = xy \cdot (z / z)$. Moreover, we will also write nothing for the reverse function composition. That means we will write RL for the function $L \circ R$. We will also apply functions more naturally. That is $L(x)$ will be written xL. For instance, given $x, y \in Q$, we have $uL_yR_x = yu \cdot x$.

2.1.2 Cayley Table

Cayley tables are a natural way to represent finite magmas. It is simply the multiplication table of a magma. Let $(M, \cdot)$ be a magma of order n. We write $M = \{x_1 \dots x_n\}$. The Cayley table of M is an $n \times n$ matrix C where $C_{i,j} = x_i \cdot x_j$. Every first-order property of a magma can be verified by a simple algorithm using the Cayley table.

Proposition 1. *Let* $(M, \cdot)$ *be a magma with elements* $\{x_1, \dots, x_n\}$*. Let*

$$(Q_i)_{1 \leq i \leq N} \in \{\forall, \exists\}^N$$

be a family of quantifiers. If $P(y_1, \dots, y_N)$ *is a propositional formula over the elements of* M *with* $y_1, \dots, y_N$ *as free variables. Then*

$$Q_1\, y_1, Q_2\, y_2, \dots, Q_N\, y_N,\ P(y_1, \dots, y_N)$$

is true in M if and only of the algorithm 1 returns true.

Algorithm 1: First order formula evaluation

```
Data:
M = {x_1, ..., x_n} elements of the magma.
Q = [Q_1, ..., Q_N] array of quantifiers.
P propositional formula with N variables.
Eval evaluation function that computes the truth value of a proposition
given a set of elements to instantiates the variables with.
Function IsTrueRecurs(i : int, Instances : array):
    if i = N then
        return Eval(P, Instances)
    end
    if Q[i] = ∀ then
        isTrue ← True;
        for j ← 1 to n do
            isTrue ← isTrue and IsTrueRecurs(i + 1, Instances + [x_j])
        end
    else
        isTrue ← False;
        for j ← 1 to n do
            isTrue ← isTrue or IsTrueRecurs(i + 1, Instances + [x_j])
        end
    end
    return isTrue
end
return IsTrueRecurs(0, [])
```

Proof. The recursive function unfolds the quantifiers, turning the universal quantifier into a "and" overall the possible elements and the existential quantifier into a "or". □

Therefore, for finite models, it makes sense to use this representation to verify the properties of the magma we study.
In the cases of loops, the axioms give us some information about the structure of the Cayley table.

Proposition 2. *Let Q be a quasigroup with elements $\{1, \dots, n\}$, and let C be its Cayley table.*

1. *C is a Latin square (each numeral appears one and only one time on each row and each column).*
2. *If Q is a loop with identity element 1, then the first row and the first column are the vector $[1, \dots, n]$.*

Proof. 1. Let fix $i \in \{1, \dots, n\}$ a row number. If $C_{i,j} = C_{i,j'}$ then by definition of the Cayley table, $i \cdot j = i \cdot j'$. By left dividing by i, we get $j = j'$. Now if $k \in \{1, \dots, n\}$, setting $j = i \setminus k$, we have $C_{i,j} = i \cdot (i \setminus k) = k$. A similar reasoning applies for the columns.

2. If 1 is the identity of the loop, then $C_{1,i} = 1 \cdot i = i = i \cdot 1 = C_{i,1}$

□

2.2 Properties

Here, we will describe some useful properties of loops that come from the definitions. Let $(Q, \cdot, 1)$ be a loop.

Proposition 3 (Inverses of the translations)**.** *Let $x \in Q$, the inverse of L_x is the left division, and the inverse of R_x is the right division. More precisely, if $y \in Q$,*

$$yL_x^{-1} = x \setminus y$$

and

$$yR_x^{-1} = y \,/\, x$$

Proof. Let $x, y \in Q$. Let u be the unique element such that $x \cdot u = y$, that is $y = uL_x$. By definition $u = x \setminus y$. But because L_x is a bijection, we also have $yL_x^{-1} = u$. This is similar for the right translation. □

This allows us to state some useful cancellation properties that are sometimes used a definition for a quasigroup.

Proposition 4. *Let $x, y \in Q$, then*

- $y = x \cdot (x \setminus y)$
- $y = x \setminus (x \cdot y)$
- $y = (y \,/\, x) \cdot x$
- $y = (y \cdot x) \,/\, x$

Proof. For the first two, we just rewrite that $y = yL_x^{-1}L_x = yL_xL_x^{-1}$ and for the last two that $y = yR_x^{-1}R_x = yR_xR_x^{-1}$. □

In particular, this shows that $x \setminus x = x \,/\, x = 1$ and $(1 \,/\, x) \cdot x = 1 = x \cdot (x \setminus 1)$. Hence, the left division of 1 by x is the right inverse of x, and the right division of 1 by x is the left inverse of x. We note x^ρ the right inverse of x and x^λ the left inverse. Hence, we have $xx^\rho = x^\lambda x = 1$. The right and left inverse do not need to be the same.

Definition 7 (Loop homeomorphism)**.** *A loop homeomorphism is a function $f : L \mapsto L'$ between two loops such that*

$$\forall x, y \in L,\ \ f(xy) = f(x)f(y)$$

Note that with this definition, we have $f(1) = 1_{L'}$ because $f(x) = f(x \cdot 1) = f(x)f(1)$ and $f(x) = f(1 \cdot x) = f(1)f(x)$. Hence $f(1)$ is the identity of L'. Like in group theory, a loop homeomorphism is injective if and only if its kernel $\ker f = \{x \in L \,|\, f(x) = 1_{L'}\}$ is reduced to $\{1_L\}$. We also have $f(x \setminus y) = f(x) \setminus f(y)$. Indeed $x \cdot (x \setminus y) = y$, by applying f on both side, we have $f(x)f(x \setminus y) = f(y)$ and we obtain the result by left-dividing by $f(x)$. We say that two loops are isomorphic if there exists some bijective homeomorphism between the two loops. Note that when we work with finite loops, injectivity (or surjectivity) is enough to prove that a homeomorphism is an isomorphism.

Definition 8 (Commutator and associator)**.** *The commutator of $x, y \in Q$ is the element $[x, y] = (yx) \setminus (xy)$. Similarly, the associator of $x, y, z \in Q$ is $[x, y, z] = (x \cdot yz) \setminus (xy \cdot z)$.*

In particular, a loop is a group if and only if for all $x, y, z \in Q$, $[x, y, z] = 1$. We clearly have:

Proposition 5. *Let $x, y, z \in Q$, we have*

- $xy = yx \iff [x, y] = 1$
- $xy \cdot z = x \cdot yz \iff [x, y, z] = 1$

Hence commutators measure how any two elements commute, and associators measure how any three elements associate.

2.3 Subloop, nucleus and center

We will describe the notion of subloop, analogous to the notion of subgroup, and construct particular subloops of interest: the nucleus and the center.

Definition 9. *A subloop S of Q is a set $S \subseteq Q$ closed under the three operations $\cdot, \backslash, /$. We note $S \leq Q$*

Proposition 6. *A subloop is a loop.*

Proof. If $\emptyset \neq S$, then let $x \in S$. $1 = x \setminus x \in S$. The restrictions of R_1 and L_1 to L are identity functions. Furthermore, the functions R_x and L_x are stable by S and so are R_x^{-1} and L_x^{-1}. That means that the right and left translations are bijections of S. □

Proposition 7. *If S is finite, S is a subloop if and only if $1 \in S$ and S is stable by multiplication.*

Proof. If S is a subloop then this is true. If S is stable by multiplication, then the restriction of R_x and L_x to S for $x \in L$ are restrictions of bijections, and are, therefore, injections. But because S is stable by multiplication, the restrictions R_x and L_x are injections from S to S and are then bijections given that S is finite. Moreover, R_1 and L_1 are identity function in S. □

We remark that any intersection of subloop is a subloop.

Definition 10 (Coset)**.** *Let $S \subseteq Q$ and $x \in Q$. The left coset xS is the set $SL_x = \{x \cdot s \,|\, s \in S\}$. The right coset Sx is the set $SR_x = \{s \cdot x \,|\, s \in S\}$.*

Definition 11 (Normal subloop)**.** *We say that the subloop $S \leq Q$ is normal, and we write $S \trianglelefteq Q$ if for every $x, y \in Q$ we have $xS = Sx$, $x(yS) = (xy)S$ and $S(xy) = (Sx)y$.*

In group theory, a subgroup is normal if $xS = Sx$ for all x, that is the left coset is always equal to the right coset. In loops, we also impose the condition that the cosets are associative (this does not mean that every element h of the normal subloop is such that $xy \cdot h = x \cdot yh$). This condition is always verified in groups because of the associativity of the law.

Definition 12 (Quotient Loop)**.** *If $S \trianglelefteq Q$, we define the quotient loop Q / S as $\{xS \,|\, x \in Q\}$ with multiplication $xS \cdot yS = (xy)S$.*

This is indeed a loop because using the fact that S is a normal subloop, we have $xS \cdot yS = Sx \cdot yS = (Sx \cdot y)S = S(xy) \cdot S = (xy)S \cdot S = (xy) \cdot SS = (xy)S$. Like in group theory, the identity element is S, and the operations do not depend on the representative of the coset.

Proposition 8. *A subloop $S \leq Q$ is normal if and only if it is the kernel of some loop homeomorphism.*

Proof. If $S \trianglelefteq Q$, then the canonical projection

$$\begin{aligned} \pi \colon Q &\to Q \,/\, S \\ x &\mapsto xS \end{aligned}$$

is a loop homeomorphism whose kernel is S. Conversely, let $S = \ker f \subseteq Q$ for some homeomorphism f. S is a subloop because f is compatible with the loop operations, so for instance if $x, y \in S$, $f(x \setminus y) = f(x) \setminus f(y) = 1 \setminus 1 = 1$. Moreover let $xs \in xS$ and set $s' = (xs)/x$. $f(s') = f(xs)/f(x) = (f(x)f(s))/f(x) = f(x)/f(x) = 1$. By right-multiplication by x, we have $xs = s'x \in Sx$. This shows $xS \subseteq Sx$. The same with left-division show that $Sx \subseteq xS$. Let $x \cdot ys \in x \cdot yS$. Set $s' = (x \cdot ys) \,/\, (xy)$. We have $f(s') = (f(x)f(y)) \,/\, (f(x)f(y)) = 1$ and $x \cdot ys = xy \cdot s'$. Similarly if $s = y \setminus (x \setminus (xy \cdot s'))$, $f(s) = f(y) \setminus (f(x) \setminus (f(x)f(y))) = 1$. Hence $x \cdot yS = xy \cdot S$. For similar reasons, $Sx \cdot y = S \cdot xy$. □

Definition 13 (Nucleus)**.** *The left nucleus of the loop Q is*

$$\mathrm{Nuc}_\lambda(Q) = \{x \in Q \,|\, \forall y, \forall z,\ [x, y, z] = 1\}$$

is the set of all elements that are left-associative. Similarly, the middle nucleus is

$$\mathrm{Nuc}_\mu(Q) = \{y \in Q \,|\, \forall x, \forall z,\ [x, y, z] = 1\}$$

and the right nucleus is

$$\mathrm{Nuc}_\rho(Q) = \{z \in Q \,|\, \forall x, \forall y,\ [x, y, z] = 1\}$$

Finally, the nucleus is the set

$$\mathrm{Nuc}(Q) = \mathrm{Nuc}_\lambda(Q) \cap \mathrm{Nuc}_\mu(Q) \cap \mathrm{Nuc}_\rho(Q)$$

Proposition 9. *Each nucleus is an associative subloop. Hence they are groups.*

Proof. Let's do the proof for the middle nucleus. We clearly have for all $x, z \in Q$, $x \cdot 1z = x \cdot z = x1 \cdot z$. If $y, y' \in \mathrm{Nuc}_\mu(Q)$, $x \cdot (yy' \cdot z) = x \cdot (y \cdot y'z) = xy \cdot (y'z) = (xy \cdot y') \cdot z = (x \cdot yy') \cdot z$. For instance, we use the fact that y was in the middle nucleus and so was middle associative with x and $y'z$. Hence the middle nucleus is stable by multiplication. If $x \in \mathrm{Nuc}_\mu(Q)$ then $x^\rho x \cdot x^\rho = x^\rho \cdot (xx^\rho) = x^\rho$. By right cancellation by x^ρ, we have $x^\rho x = 1$. That means $x^\rho = x^\lambda$. Each element in the middle nucleus has a unique left and right inverse x^{-1}. To proves that it is a subloop, we now need to show that for all $x, y \in \mathrm{Nuc}_\mu(Q)$, both $y \setminus x = xL_y^{-1}$ and $x \,/\, y = xR_y^{-1}$ are in $\mathrm{Nuc}_\mu(Q)$. But if $y \in \mathrm{Nuc}_\mu(Q)$ for any $a \in Q$, $aR_yR_{y^{-1}} = ay \cdot y^{-1} = a \cdot yy^{-1} = a$. That means $R_yR_{y^{-1}}$ is the identity function, so $R_{y^{-1}} = R_y^{-1}$. similarly, $L_{y^{-1}} = L_y^{-1}$. If we show that for any $y \in \mathrm{Nuc}_\mu(Q)$, y^{-1} is also in $\mathrm{Nuc}_\mu(Q)$, then $y \setminus x = xL_y^{-1} = xL_{y^{-1}}$ and $x \,/\, y = xR_y^{-1} = xR_{y^{-1}}$ would also be in the middle nucleus because it is stable by multiplication. So let's take $x \in \mathrm{Nuc}_\mu(Q)$ and show that $x^{-1} \in \mathrm{Nuc}_\mu(Q)$. Let $a, b \in Q$. We can write $a = tx$ with $t = a/x$. Now $ax^{-1} \cdot b = (tx)x^{-1} \cdot b = (t \cdot xx^{-1}) \cdot b$ because x is in $\mathrm{Nuc}_\mu(Q)$. So $ax^{-1} \cdot b = tb$. And $a \cdot x^{-1}b = tx \cdot x^{-1}b = t \cdot x(x^{-1}b) = t \cdot bL_x^{-1}L_x = tb$. Thus, x^{-1} is in the middle nucleus. Moreover, if x,y,$z \in \mathrm{Nuc}_\mu(Q)$ we have $x \cdot yz = xy \cdot z$ because in particular, y is in the middle nucleus. Hence, $\mathrm{Nuc}_\mu(Q)$ is an associative subloop, it is a group. Similar reasoning could show that $\mathrm{Nuc}_\lambda(Q)$ and $\mathrm{Nuc}_\rho(Q)$ are also associative subloops. Finally, $\mathrm{Nuc}(Q)$ is an associative subloop as intersection of associative subloops. □

Definition 14 (Center)**.** *The commutant of Q is the set $C(Q) = \{x \in Q \,|\, \forall y \in Q,\ xy = yx\}$.*
The center of Q is $Z(Q) = \mathrm{Nuc}(Q) \cap C(Q)$

Proposition 10. *The center of a loop is a normal subloop.*

Proof. Because the elements commute, we have $xZ(Q) = Z(Q)x$. Because the elements of the center are also in the nucleus, they are associative and then $x \cdot yZ(Q) = (xy) \cdot Z(Q)$ and $Z(Q)x \cdot y = Z(Q) \cdot (xy)$. □

3 Multiplication and inner mapping groups

When one wants to study a group G, it is often useful to consider $\mathrm{Aut}(G)$, the group of automorphisms of G. This is an interesting subgroup of the bijection of G and in particular, it has a normal subgroup $\mathrm{Inn}(G) = \{x \mapsto g^{-1}xg \mid g \in G\}$, the inner automorphisms group. In loop theory, the inverse g^{-1} is not well defined, but we still can use an analogous inner mapping group through a definition that involves left and right translation. Like in group theory, studying this group allows us to prove interesting things about the loop it comes from. For instance, the AIM conjecture tries to relate the nilpotency class of a loop and the nilpotency class of its inner mapping group. Furthermore, the inner mapping group of Q fully characterizes the normal subloops of Q, and the center of a loop can be studied through the center of its multiplication group.

3.1 Definition

Let $(Q, \cdot, 1)$ be a loop and consider, for any $x, y \in Q$, the following mappings

$$\begin{aligned} T_x &= R_x L_x^{-1} \\ L_{x,y} &= L_x L_y L_{yx}^{-1} \\ R_{x,y} &= R_x R_y R_{xy}^{-1} \\ M_{x,y} &= R_y L_x R_{xy}^{-1} \end{aligned}$$

Definition 15 (Multiplication group and inner mapping group)**.** *The multiplication group* $\mathrm{Mlt}(Q)$ *is the subgroup of the bijections of* Q *generated by all the left and right translations. That is*

$$\mathrm{Mlt}(Q) = \langle L_x, R_x,\ x \in Q \rangle$$

The inner mapping group is the subgroup of $\mathrm{Mlt}(Q)$ *generated by* $M_{x,y}$ *and* $R_{x,y}$*. That is*

$$\mathrm{Inn}(Q) = \langle M_{x,y}, R_{x,y},\ x, y \in Q \rangle$$

Theorem 1. *Each element* $\phi \in \mathrm{Mlt}(Q)$ *has a unique representation* UR_x *with* $U \in \mathrm{Inn}(Q)$ *and* $x \in Q$*. Moreover,* $x = 1\phi$*.*

Proof. First, we see that $1M_{x,y} = xy \,/\, xy = 1$ and $1R_{x,y} = xy \,/\, xy = 1$, so we have $1U = 1$ for all $U \in \mathrm{Inn}(Q)$. For the uniqueness, if $\phi = UR_x$, then $1\phi = 1UR_x = 1R_x = x$ so x is uniquely determined. Moreover, $U = \phi R_x^{-1}$ and so U is also uniquely determined. Now, we show that any $\phi \in \mathrm{Mlt}(Q)$ has such a representation. For that, we consider the seven following identities that hold for all $x, y \in Q$:

$$R_x R_y = R_{x,y} R_{xy} \tag{1}$$
$$R_x L_y = M_{y,x} R_{yx} \tag{2}$$
$$R_x R_y^{-1} = R_{p,y}^{-1} R_p \text{ with } p = x R_y^{-1} \tag{3}$$
$$R_x L_y^{-1} = M_{y,q}^{-1} R_q \text{ with } q = x L_y^{-1} \tag{4}$$
$$L_x = M_{x,1} R_x \tag{5}$$
$$R_x^{-1} = R_{u,x}^{-1} R_u \text{ with } u = 1R_x^{-1} \tag{6}$$
$$L_x^{-1} = M_{x,v}^{-1} R_v \text{ with } v = 1L_x^{-1} \tag{7}$$

For instance we will prove 4. $M_{y,q} = M_{y,y\backslash x} = R_{y\backslash x} L_y R^{-1}_{y\cdot(y\backslash x)} = R_{y\backslash x} L_y R_x^{-1}$. So $M^{-1}_{y,q} R_q = R_x L_y^{-1} R^{-1}_{y\backslash x} R_{y\backslash x} = R_x L_y^{-1}$. We can also deduce the last three from 2, 3 and 4 setting $x = 1$. Now, from the definition of $\mathrm{Mlt}(Q)$, if $\phi \in \mathrm{Mlt}(Q)$ then there exist an integer $r \geq 1$ such that $\phi = \phi_1 \dots \phi_r$ with $\phi_i \in \{L_x, R_x, L_x^{-1}, R_x^{-1} \,|\, x \in Q\}$. We will prove the existence by induction over r. If $r = 1$, the decomposition follows from 5, 6 and 7. By induction, we assume it has been proven for all product of r factors or less. If $\phi = \phi_1 \dots \phi_r \phi_{r+1}$ then by induction hypothesis, $\phi = V R_x \phi_{r+1}$ with $x \in Q$ and $V \in \mathrm{Inn}(Q)$. But using the previous identities, we can rewrite $R_x \phi_{r+1}$ as $W R_y$ with $W \in \mathrm{Inn}(Q)$ and $y \in Q$. That is, $\phi = VW R_y = U R_y$ with $U = VW \in \mathrm{Inn}(Q)$. Finally, $1\phi = 1U R_x = 1R_x = x$ because $U \in \mathrm{Inn}(Q)$ so $1U = 1$. □

3.2 Properties

The theorem 1 has interesting corollaries about the inner mapping group.

Corollary 1. *The inner mapping group is the subgroup of* $\mathrm{Mlt}(Q)$ *that fixes* 1. *More precisely,*

$$\mathrm{Inn}(Q) = \{\phi \in \mathrm{Mlt}(Q) \,|\, 1\phi = 1\}$$

Proof. If $1\phi = 1$, by theorem 1, $\phi = U R_x$ with $U \in \mathrm{Inn}(Q)$ and $x = 1\phi = 1$. So $\phi = U R_1 = U\,\mathrm{Id} = U \in \mathrm{Inn}(Q)$. Conversely, we saw that if $U \in \mathrm{Inn}(Q)$ then $1U = 1$. □

Corollary 2. *If* Q *is finite,* $|Q| = [\mathrm{Mlt}(Q) : \mathrm{Inn}(Q)]$

Proof. Each coset $\mathrm{Inn}(Q)\phi$ with $\phi \in \mathrm{Mlt}(Q)$ can be written as $\mathrm{Inn}(Q)R_x$ because $\phi = U R_x$ with $U \in \mathrm{Inn}(Q)$. The x is unique because if $\mathrm{Inn}(Q)R_x = \mathrm{Inn}(Q)R_y$ then in particular $R_x = U R_y$ so $U = \mathrm{Id}$ and $R_x = R_y$ by unicity of the decomposition in theorem 1. And every $x \in Q$ is attained with the coset $\mathrm{Inn}(Q)R_x$. Thus there is a bijection between the coset of $\mathrm{Inn}(Q)$ in $\mathrm{Mlt}(Q)$ and the elements of Q. □

Corollary 3. *Every element* $\phi \in \mathrm{Mlt}(Q)$ *has an unique representation* $\phi = V L_x$ *with* $V \in \mathrm{Inn}(Q)$ *and* $x = 1\phi \in Q$.

Proof. Let $\phi \in \mathrm{Mlt}(Q)$ and $x = 1\phi$. Set $V = \phi L_x^{-1}$. We have $1V = 1\phi L_x^{-1} = x L_x^{-1} = 1$ so $V \in \mathrm{Inn}(Q)$ and we have $\phi = V L_x$. $x = 1\phi$ is uniquely determined so V is also uniquely determined, hence the uniqueness of the decomposition. □

We can also generate the inner mapping group by various sets of generators. For instance, here is a theorem that exhibits another generating set.

Theorem 2. $\mathrm{Inn}(Q) = \langle T_x, L_{x,y}, R_{x,y} \,|\, x,y \in Q \rangle$.

Proof. We note $F = \langle T_x, L_{x,y}, R_{x,y} \,|\, x,y \in Q \rangle$ Because $1T_x = 1L_{x,y} = 1R_{x,y} = 1$, F is included in $\mathrm{Inn}(Q)$. Now consider the set

$$K = \{\beta \in \mathrm{Mlt}(Q) \,|\, \beta \in F \cdot R_{1\beta}\}$$

If we set $t = 1\beta$, we have for every $x \in Q$, $1\beta R_x = tx$. Hence, for every $\beta \in K$, there exists $\phi \in F$ such that $\beta = \phi R_{1\beta} = \phi R_t$. So

$$\beta R_x = \phi R_t R_x = \phi R_{t,x} R_{tx} = \phi R_{t,x} R_{1\beta R_x}$$

By calling $\gamma = \beta R_x$, the last equality become

$$\gamma = \phi R_{t,x} R_{1\gamma}$$

But ϕ and $R_{t,x}$ are in F, so $\gamma \in K$, i.e. $\beta R_x \in K$. This is true for all $x \in Q$. Similarly, we can show that βL_x, βR_x^{-1} and βL_x^{-1} are in K. Hence $K\,\mathrm{Mlt}(Q) \subseteq K \subseteq \mathrm{Mlt}(Q) \subseteq K\,\mathrm{Mlt}(Q)$, so $K = \mathrm{Mlt}(Q)$. So in particular, $\mathrm{Inn}(Q) \subseteq K$. So if $\beta \in \mathrm{Inn}(Q)$, $\beta = \phi R_{1\beta}$ for some $\phi \in F$. But $1\beta = 1$ and $R_{1\beta} = I$. So $\beta = \phi \in F$. □

We can also relate the center of a loop with the center of its multiplication group.

Theorem 3. *$Z(Q)$ is isomorphic to $Z(\mathrm{Mlt}(Q))$.*

See [12] pp25 for a proof.

3.3 Inner mapping and normal subloop

Now, we will explore how knowledge about the multiplication group and the inner mapping group can be used to determine if a given subloop of Q is normal.

Lemma 1. *Let $S \leq Q$. If $S \trianglelefteq Q$ then $S\,\mathrm{Inn}(Q) = \mathrm{Inn}(Q)$. That is, S is stable by any inner mapping.*

Proof. It suffices to show that this is true for the generators of the inner mapping group. Let $x, y \in Q$. We have

$$SR_xL_x^{-1} = Sx \cdot L_x^{-1} = x \setminus (Sx) = x \setminus (xS) = (x \setminus x)S = S$$

because S is a normal subloop. Moreover,

$$SL_{x,y} = (y \cdot xS)L_{yx}^{-1} = (yx)\ ((yx)S) = (yx \setminus yx)S = S$$

and finally

$$SR_{x,y} = (Sx \cdot y)R_{xy}^{-1} = (S(xy)) \,/\, xy = S(xy \,/\, xy) = S$$

. □

This necessary condition is sufficient. This is the content of the following theorem.

Theorem 4. *Let $S \leq Q$. $S \trianglelefteq Q$ if and only if $S\,\mathrm{Inn}(Q) = \mathrm{Inn}(Q)$.*

Proof. We saw that the condition was sufficient in the lemma 1. Before doing the proof, we shall remark that for any $a \in Q$ and any $\phi \in \mathrm{Mlt}(Q)$, we have $a\phi = aU \cdot x = x \cdot aV$ for some $U, V \in \mathrm{Inn}(Q)$ and $x = 1\phi$. Indeed, from theorem 1, $\phi = UR_x$, so $1\phi = 1UR_x = 1R_x = x$ because $1U = 1$ when $U \in \mathrm{Inn}(Q)$. If $S\,\mathrm{Inn}(Q) = \mathrm{Inn}(Q)$ then $SL_xR_x^{-1} = S$ because $1L_xR_x^{-1} = x \,/\, x = 1$ i.e. $L_xR_x^{-1} \in \mathrm{Inn}(Q)$. Hence, $SLx = SRx$, or $xS = Sx$. Moreover, $L_{x,y} \in \mathrm{Inn}(Q)$ so $SL_{x,y} = S$ or $SL_xL_yL_{yx}^{-1} = S$ so $y{\cdot}xS = yx{\cdot}S$. And similarly, $SR_{x,y} = S$ implies $Sx{\cdot}y = S{\cdot}xy$. Hence $S \trianglelefteq Q$. □

Finally, let us remark that this notion of inner mapping group corresponds to the inner automorphism of groups.

Proposition 11. *If G is a group, then $\mathrm{Inn}(G)$ is the group of inner automorphism of G.*

Proof. By theorem 2, $\mathrm{Inn}(G) = \langle T_x, L_{x,y}, R_{x,y} \,|\, x,y \in Q \rangle$. But, in a group $L_{x,y} = L_xL_yL_{yx}^{-1} = L_{yx}L_{yx}^{-1} = \mathrm{Id}$ and similarly $R_{x,y} = \mathrm{Id}$. Moreover the T_x are exactly the inner automorphism $g \mapsto x^{-1}gx$. So $\mathrm{Inn}(G)$ is the group generated by all the inner automorphisms. But they already form a group so $\mathrm{Inn}(G)$ is the group of inner automorphisms. □

4 The AIM conjecture

The goal of this section is to state the AIM conjecture and one of its weaker versions that we will work with later in the thesis. An AIM loop is a loop whose inner mapping group is abelian. In this case, the conjecture states that the nilpotency class of the loop should be at most three. The concept of nilpotency for loops generalizes the nilpotency of groups, but it is not possible to connect the inner mapping group of a loop with the loop itself easily. The AIM conjecture tries to give a partial answer to this problem. Even though it is not proved in the most general case, some specific kinds of loops have a positive answer to this problem.

4.1 Nilpotency class of loops

The nilpotency of an algebraic structure is a way to measure the degree of commutativity of this structure. With this tool, let us say in group theory, a group is abelian if and only if its nilpotency class is equal to one. If it is equal to two, then it is almost commutative in the sense that the group factored by its center $G/Z(G)$ is commutative. The nilpotency class of a group can be seen as the length of a chain of successive factor groups constructed in a certain way. This definition can be generalized in loop theory because, fortunately, the subloops we will consider will be normal. This will be the definition of *central nilpotence*. However, there is another generalization of the nilpotence in group theory. This is called the *supernilpotence*. It comes from abstract considerations in universal algebra and will not be discussed in this thesis. While in group theory, the notion of central nilpotence and supernilpotence are the same, it is not true anymore in loop theory. One as to specify what kind of nilpotence they are talking about. More details about this distinction can be found in [14]

Let $(Q, \cdot, 1)$ be a loop. Recall that $Z(Q)$ is the center of Q, the elements that commute and associate with every element of the loop. The center is a normal subloop.

Definition 16 (Upper Central Series)**.** *The upper central series of Q is the sequence $(Z^n(Q))_{n\in\mathbb{N}}$ where $Z^n(Q)$ is defined by induction as follow:*

1. *$Z^0(Q) = \{1\}$ the trivial subloop*
2. *$Z^{n+1}(Q) = \pi^{-1}\left(Z(Q \,/\, Z^n(Q))\right)$ where $\pi : Q \mapsto Q \,/\, Z^n(Q)$ is the canonical projection.*

In other words, the next element in the upper central series is the preimage via the canonical projection of the center of the loop factored by the previous element in the series.

Definition 17. *We say that a loop is nilpotent if there exists $n \in \mathbb{N}$ such that $Z^n(Q) = Q$. In this case, we call the nilpotency class of Q the natural number $n = \min\{m \,|\, Z^m(Q) = Q\}$. We write $\mathrm{cl}(Q) = n$*

We remark that the only group of nilpotency class 0 is the trivial group.

Proposition 12. *If a loop is nilpotent of class 1, then it is an abelian group.*

Proof. By definition, $Q = Z^1(Q) = \pi^{-1}\left(Z(Q \,/\, \{1\})\right)$. But $Q \cong Q \,/\, \{1\}$ via the canonical projection π, and so $Z(Q) \cong Z(Q \,/\, \{1\}) \cong Q$. Q is isomorphic to its center, that means it is it whole center and therefore $Q = Z(Q)$ so Q is associative an commutative, it is an abelian group. □

Here we have to be careful. In group theory, a group is nilpotent of class 1 if it is a commutative group. In loop theory, we do not have that a loop is nilpotent of class 1 if it is a commutative loop. A loop is nilpotent of class 1 if it is an abelian group, i.e. a commutative and associative loop.

For instance, consider the loop Q with the following Cayley table:

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	3	6	5
3	3	4	5	6	1	2
4	4	3	6	5	2	1
5	5	6	2	1	3	4
6	6	5	1	2	4	3

Some computation shows that the center of this loop is the set $\{1, 2\}$. Hence $Z^1(Q) = \{1, 2\}$. The factor loop $Q \,/\, \{1, 2\}$ is an abelian group, so its center is itself and thus $Z^2(Q) = \pi^{-1}\left(Z(Q \,/\, Z^1(Q))\right) = \pi^{-1}\left(Q \,/\, Z^1(Q)\right) = Q$. So $\mathrm{cl}(Q) = 2$.

4.2 The AIM conjecture

Definition 18. *We say that a loop is AIM if its inner mapping group is abelian.*

In the previous example, a call to GAP [6] tells us that $\mathrm{Mlt}(Q) = \mathbb{Z}_2 \times A_4$ where A_4 is the alternating group of degree 4. It has size $2 \times 12 = 24$. Meanwhile, the inner mapping group is $\mathrm{Inn}(Q) = \mathbb{Z}_2 \times \mathbb{Z}_2$. That means that the loop Q is AIM. In fact, as we will see later, every loop of nilpotency class two is AIM (we also can see that $[\mathrm{Mlt}(Q) : \mathrm{Inn}(Q)] = 24/4 = 6 = |Q|$ as expected). In group theory, we have the following results:

Lemma 2. *If G is a group then* $\mathrm{Inn}(G) \cong G \,/\, Z(G)$

Proof. We note ψ_x the inner automorphism $u \mapsto x^{-1}ux$. Consider the mapping

$$\begin{aligned} f \colon G &\to \mathrm{Aut}(G) \\ x &\mapsto \psi_x \end{aligned}$$

We have $\psi_x\psi_y = \psi_{xy}$ because $u\psi_x\psi_y = (x^{-1}ux)\psi_y = y^{-1}x^{-1}uxy = (xy)^{-1}uxy = u\psi_{xy}$. That means f is a morphism and we see that $f(G) = \mathrm{Inn}(G)$. $x \in \ker f$ if and only if for all $u \in G$, $x^{-1}ux = u$ if and only if $x \in Z(G)$. The center of G is precisely the kernel of f. By the first isomorphism theorem, $G \,/\, Z(G) = G \,/ \ker f \cong f(G) = \mathrm{Inn}(G)$. □

Moreover, as a consequence, we have the following theorem:

Theorem 5. *If G is a group,* $\mathrm{cl}(\mathrm{Inn}(G)) \leq n$ *if and only if* $\mathrm{cl}(G) \leq n + 1$.

A rigorous proof can be found in [2] but the insight is to remark that $\mathrm{cl}(\mathrm{Inn}(g)) = \mathrm{cl}(G \,/\, Z(G))$ and because of the way the upper series is constructed, the series for $G \,/\, Z(G)$ is like the series for G but shifted by one because $G \,/\, Z(G) = G \,/\, Z^1(G)$. While this result is true for groups, neither of the two implications generalize to loops. For instance, there exist loops of nilpotency class 3 and an inner mapping that is not nilpotent [7]. For the other implication, counterexamples are, for instance, loops of Csörgő type that we will study later. The AIM conjecture is an attempt to generalize the previous theorem to loops in the case where $n = 1$, i.e. when $\mathrm{Inn}(Q)$ is nilpotent of class 1, i.e. is abelian. Indeed, specializing the theorem for $n = 1$, we obtain:

Corollary 4. *If G is a group,* $\mathrm{cl}(\mathrm{Inn}(G))$ *is abelian if and only if* $\mathrm{cl}(G) \leq 2$.

The initial version of the AIM conjecture was the hope that the corollary 4 holds for loops. That is, if a loop is AIM if and only if its nilpotency class is at most 2. We will see that one implication hold, if a loop is nilpotent of class at most 2, then its inner mapping group is abelian. However, in 2004 Piroska Csörgő constructed loops of nilpotency class 3 and with an abelian inner mapping, which is a counterexample to the first AIM conjecture. This thesis aims to study in more detail those kinds of loops, called loops of Csörgő type. But for now, we will study in more detail a refined version of the AIM conjecture:

Conjecture 1 (Main AIM conjecture)**.** *If Q is an AIM loop, then Q / $\mathrm{Nuc}(Q)$ is an abelian group and Q / $Z(Q)$ is a group. In particular,* $\mathrm{cl}(Q) \leq 3$.

For this conjecture to make sense, we need the following proposition, which will allow us to factor the loop by its nucleus.

Proposition 13. *If Q is AIM, then* $\mathrm{Nuc}(Q)$ *is a normal subloop.*

Proof. We will use theorem 4 and prove that for every generator of theorem 2, the result is still in the nucleus. Let $u \in \mathrm{Nuc}(Q)$ and $x,y,z \in Q$, we have $uL_xL_y = uL_{yx}$ because $u \in \mathrm{Nuc}_\rho(Q)$. Hence $uL_{x,y} = u$. Similarly, $u \in \mathrm{Nuc}_\lambda(Q)$ so $uR_{x,y} = u$. We'd now like to show that uT_x is in the nucleus, but $uT_x = uL_{y,z}T_x = uT_xL_{y,z}$ because the inner mapping group is abelian. that is $uT_x = uT_xL_yL_zL_{zy}^{-1}$ i.e.

$$zy \cdot uT_x = z \cdot y(uT_x)$$

so $uT_x \in \mathrm{Nuc}_\rho(Q)$. The exact same reasoning with $R_{y,z}$ show that $uT_x \in \mathrm{Nuc}_\lambda(Q)$. Now consider $S = L_yR_zL_y^{-1}R_z^{-1}$. We have $1S = 1$ so $S \in \mathrm{Inn}(Q)$, therefore $uT_xS = uST_x$. Moreover, $u \in \mathrm{Nuc}_\mu(Q)$ so $uL_rR_z = uR_zL_z$ and then $uS = uR_zL_yL_y^{-1}R_z^{-1} = uR_zR_z^{-1} = u$. Hence $uT_xS = uT_x$ i.e. $uT_xL_yR_z = uTxR_zL_y$, that is $uT_x \in \mathrm{Nuc}_\mu(Q)$. Thus, $uT_x \in \mathrm{Nuc}(Q)$. □

There are some positive results about the conjecture. For instance, Niemenmaa and Kepka proved in [11] that:

Theorem 6. *If* $\mathrm{Inn}(Q)$ *is nilpotent, then Q is nilpotent.*

However, this result puts no bound on the nilpotency class of the loop. The AIM conjecture put a precise upper bound of 3 when the bound on the inner mapping group is 1. Bruck also proved in [1] a the reciprocal of corollary 4 that is:

Theorem 7. *If* $\mathrm{cl}(Q) \leq 2$*, then Q is an AIM loop.*

In the next section of this thesis, we will focus on the following weaker version of the AIM conjecture:

Conjecture 2 (Weak AIM conjecture)**.** *If Q is AIM, then* $\mathrm{cl}(Q) \leq 3$.

This statement follows from the main version skipping directly to the "in particular" case. More detail can be found in [9].

4.3 When the AIM conjecture is true

During summer 2021, it has been announced that the weak version conjectured in 2 was proven, but no paper was published yet as I am writing those lines. However, let us review particular class of loops where the AIM conjecture hold.

Definition 19 (LC Loop)**.** *A loop is said LC if it satisfies any of the following equivalent identities:*

$$\begin{aligned} x(x \cdot yz) &= (x \cdot xy)z \\ x(x \cdot yz) &= (xx \cdot y)z \\ xx \cdot yz &= (x \cdot xy)z \\ x(y \cdot yz) &= (x \cdot yy)z \end{aligned}$$

The equivalence and more properties about the LC loops can be found in [13]. In [9], we learn that the main AIM conjecture is true for LC loops and that the authors suspect that the corollary 4 holds for LC loop, hence, the inner mapping group is abelian if and only if the loop is nilpotent of class less than two.
Another important and well-studied type of loop is Moufang loops.

Definition 20. *A loop Q is said Moufang if any of the following equivalent identities hold for all $x, y, z \in Q$:*

$$\begin{aligned} z(x \cdot zy) &= (zx \cdot z)y \\ x(z \cdot yz) &= (xz \cdot y)z \\ zx \cdot yz &= (z \cdot xy)z \\ zx \cdot yz &= z(xy \cdot z) \end{aligned}$$

Moufang loops can be seen as loops with a weaker version of associativity. The Main AIM conjecture is true for Moufang loops [9]. However, unlike LC loops, there is an AIM Moufang loops of order 2^{14} with nilpotency class 3 [10]. Other varieties of loops satisfy the AIM conjecture. We can cite *extra loops*, *automorphic loops*, *CC loops*, etc [9]. This explains why the AIM conjecture is believed to be true [8].

5 Construction of Csörgő loops

In this section, we will focus on a particular type of AIM loop, the Csörgő type loop, or Csörgő loop. Those are AIM loops with nilpotency class strictly greater than 2. The first Csörgő loop was discovered by Csörgő in 2004 and its construction can be found in [3]. It was the first counterexample to the first version of the AIM conjecture, that is the corollary 4, but for loops. Therefore Csörgő loops are an interesting class of loops, and open problems concern them. Among them is the following question: are there any Csörgő loops of order less than 128? We will see how we tried to answer this question later in the thesis. For now, we will focus on an existing construction of Csörgő loops.
We will reproduce the strategy used in [5]. We will start from a product of groups of nilpotency class 2 by $\mathbb{Z}_2$ and we will modify the multiplication law of the result according to some trilinear alternating form, giving rise to a loop with commuting inner mapping group and nilpotency class 3. Later, we will reverse-engineer the construction using GAP to help us generate smaller Csörgő loops.

5.1 The strategy

The strategy involves group theoretical concepts that require some definitions:

Definition 21. *If H is a group, the derived subgroup H' of H is the smallest normal subgroup of H such that H/H' is abelian. It is the subgroup $H' = \langle [u,v],\ u,v \in H \rangle$.*

Definition 22. *Let p be a prime number. A group G is an elementary abelian p-group if any element of G has an order of p*

For instance, $\mathbb{Z}_p^n$ is an elementary abelian p-group for all $n \geq 1$. In fact, by the classification of finite abelian groups, those are exactly the finite elementary abelian p-groups. Moreover, because $\mathbb{Z}_p$ is also the field $\mathbb{F}_p$, we can see and elementary abelian p-group $\mathbb{Z}_p^n$ as a vector space of dimension n over $\mathbb{F}_p$.

Consider the abelian group $A = \{-1, 1\}$, it is $\mathbb{Z}_2$ with multiplicative notation. Let H a group of nilpotency class 2 such that:

- $H' = Z(H)$
- $H \,/\, H'$ is an elementary abelian 2-group with basis $\{e_1H', \ldots, e_dH'\} \cong \mathbb{Z}_2^d$
- H' is also an elementary abelian 2-group with basis $\{[e_i, e_j] \,|\, 1 \leq i,j \leq d\}$ ($[x,y] = x^{-1}y^{-1}xy$ in the case of groups)

Moreover, we consider $f = \det$ the determinant of the $(H \,/\, H')^3$ seen as a $A \cong \mathbb{F}_2$ vector space of dimension 3. f is a symmetric trilinear alternating form. To avoid cumbersome notation, we will write $f(uH', vH', wH') = f(u,v,w)$ for any $u,v,w \in H$. The goal is to construct $\mu, \delta : H \times H \to A$ such that for any $u,v,w \in H$, $f(u,v,w) = \delta([u,v],w)$ and $\delta(u,v) = \mu(u,v)\mu(v,u)^{-1}$ with the additional properties:

- $\mu(uv,w) = \mu(u,w)\mu(v,w)^{-1}$ if $\{u,v,w\} \cap H' \neq \emptyset$
- $\mu(u,vw) = \mu(u,v)\mu(u,w)^{-1}$ if $\{u,v,w\} \cap H' \neq \emptyset$

Using an alternating form yields $\delta([w,v],u) = \delta([w,u],v)^{-1}$ which is the condition that ensures that the inner mapping group is abelian provided that the previous

equalities hold for μ. Now, consider the product group $(A \times H, \cdot)$ and construct the magma $Q = (A \times H, \star)$ such that for any $(a, h), (a', h') \in Q$,

$$(a, h) \star (a', h') = (aa'\mu(h, h'), hh')$$

Then, according to [5], Q is a loop with commuting inner mapping and nilpotency class 3.

5.2 Constructing δ

Let $M = H'$ and $T = \{t_1, \ldots, t_k\}$ with $t_1 = 1$ be a transversal set for M in H, that is a set such that every coset of M contains exactly one t_i. This allows us to decompose each element $u \in H$ in a unique way $u = mt$ with $m \in M$ and $t \in T$. The construction goes as follow: we first fix δ on $M \times H$ using the fact that M is generated by the commutator and that we must have $f(u, v, w) = \delta([u, v], w)$. We then extend δ to $H \times H$ using the decomposition $u = mt$.
Let $1 \leq i, j \leq k$ and let $u \in H$. We have $1 \leq k \leq d$ and $m \in M$ such that $u = e_k m$. then set

$$\delta([e_i, e_j], e_k m) = f(e_i, e_j, e_k)$$

using the fact that $([e_i, e_j])_{1 \leq i,j \leq d}$ is a basis of M, we can extend δ into a linear mapping from $M \times H$ to A. That is $\delta(m_1 m_2, u) = \delta(m_1, u)\delta(m_2, u)$. Moreover, if $u_1 = e_i m_1$ and $u_2 = e_j m_2$ then $u_1 u_2 = (e_i e_j) m_3$ because M is a normal subgroup of H. Hence

$$\delta(m, u_1 u_2) = f(e, e', e_i e_j) = f(e, e', e_i e_j) = f(e, e', e_j) = \delta(m, u_1)\delta(m, u_2)$$

This argument extends δ into a linear mapping in its second variable for all $u \in H$ because f is linear. We also can see that for all $m, m' \in M$, we have $\delta(m, m') = 1$ because the third argument of f is the identity of H according to the unicity of the decomposition of m'. Then f vanishes because one of its arguments is trivial.

Lemma 3. *If a group G is such that $\mathrm{cl}(G) \leq 2$ then $x \mapsto [x, y]$ and $x \mapsto [y, x]$ are endormorphisms for all $y \in G$.*

Proof. Because $\mathrm{cl}(G) \leq 2$, $G \,/\, Z(G)$ is abelian and hence by definition of G', $G' \leq Z(G)$. In particular, all commutators are in $Z(G)$. Now let $x, y, z \in G$. See that:

$$[x, yz] = x^{-1}z^{-1}y^{-1}xyz = x^{-1}z^{-1}xzz^{-1}x^{-1}y^{-1}xyz = [x, z]z^{-1}[x, y]z$$

but $[x, y] \in Z(G)$ so $[x, yz] = [x, z][x, y]z^{-1}z = [x, z][x, y]$. Now

$$[xy, z] = [z, xy]^{-1} = ([z, x][z, y])^{-1} = [y, z][x, z] = [x, z][y, z]$$

the last equality being justified by the fact that any commutator commutes. □

Lemma 4. *For every $u, v, w \in H$ we have $\delta([u, v], w) = f(u, v, w)$*

Proof. First, $[u, v] \in M$ because it is the subgroup generated by the commutators. Second, $u = e_1^{u_1} \ldots e_d^{u_d} m$ and $v = e_1^{v_1} \ldots e_d^{v_d} m'$ for some $u_i, v_i \in \{0, 1\}$ because each $t \in T$ can be written a a product of power of e_1 and $e_i^2 = 1$ because $H \,/\, H'$ is a 2-group with basis $\{e_1 H', \ldots e_d H'\}$. Using the lemma 3, and the linearity of δ on its first component, we get:

$$\delta([u, v], w) = \delta\left(\prod_{i \neq j} [e_i^{u_i}, e_j^{v_j}], w\right) \delta([m, m'], w) = \prod_{i \neq j} \delta([e_i^{u_i}, e_j^{v_j}], w)$$

note that when $i = j$, the commutator $[e_i^{u_i}, e_j^{v_j}]$ is trivial and $\delta([m, m'], w) = f(1, 1, \cdot)$ is also trivial. Moreover, f is trilinear and alternating so:

$$f(u, v, w) = \prod_{i \neq j} f(e_i^{u_i}, e_j^{v_j}, w)$$

this is justified by the fact that $f(m, m', w) = 1$ because recall that this is a shorthand for $f(mM, m'M, wM)$ and $mM = m'M$. Finally, we verify that

$$f(e_i^{u_i}, e_j^{v_j}, w) = \delta([e_i^{u_i}, e_j^{v_j}], w)$$

using the definition of δ. □

To extend δ to $H \times H$, we use the transversal set T to define:

- $\delta(t_1, t_j) = 1$ for every $j \in \{1, \ldots, k\}$
- $\delta(t_i, t_j)$ arbitrary when $1 \leq i < j \leq k$
- $\delta(t_j, t_i) = \delta(t_i, t_j)^{-1}$ when $1 \leq i < j \leq k$
- $\delta(t_i, t_i) = 1$ for every $i \in \{1, \ldots, k\}$

Hence, if $h, h' \in H$, we can decompose $h = mt$ and $h' = m't'$ with $m, m' \in M$ and $t, t' \in T$ and define:

$$\delta(mt, m't') = \delta(m, t')\delta(m', t)^{-1}\delta(t, t')$$

where all the quantities have been defined previously. One can check that this extends $\delta : M \times H \mapsto H$.

Lemma 5. *The map $\delta : H \times H \mapsto A$ satisfies for every $u, v \in H$ and $m \in M$:*

1. $\delta(u, v) = \delta(v, u)^{-1}$
2. $\delta(u, mv) = \delta(u, m)\delta(u, v)$
3. $\delta(u, vm) = \delta(u, v)\delta(u, m)$
4. $\delta(m, uv) = \delta(m, u)\delta(m, v)$

The verification, as well as more detail on the construction of δ, can be found in [5]

5.3 Constructing μ

We keep the same notation as in the previous section. We will first define μ on $M \cup T \times M \cup T$ with the following:

- $\mu(t_1, t_1) = 1$
- $\mu(t_i, t_i)$ arbitrary for $1 < i \leq k$
- $\mu(t_i, t_j) = \delta(t_i, t_j)$ $1 \leq i < j \leq k$
- $\mu(t_j, t_i) = 1$ if $1 \leq i < j \leq k$

Furthermore, for any $m, n \in M$ and $t \in T$

- $\mu(m, n) = 1$

- $\mu(m,t) = \delta(m,t)$
- $\mu(t,m) = 1$

We can now extend μ to $H \times H$ with

$$\mu(mt, m't') = \mu(m,t')\mu(t,t')$$

Theorem 8. *For every $u, v \in H$ and $m \in M$, we have*

$$\delta(u,v) = \mu(u,v)\mu(v,u)^{-1}$$

Furthermore, the following identities hold:

1. $\mu(mu, v) = \mu(m,v)\mu(u,v)$
2. $\mu(um, v) = \mu(u,v)\mu(m,v)$
3. $\mu(uv, m) = \mu(u,m)\mu(v,m)$
4. $\mu(u, mv) = \mu(u,m)\mu(u,v)$
5. $\mu(u, vm) = \mu(u,v)\mu(u,m)$
6. $\mu(m, uv) = \mu(m,u)\mu(m,v)$

The verifications are once again made in [5]. This construction is the one we needed because each identity in theorem 8 represents the six cases that can happen in the additional properties required for μ defined earlier.

5.4 Resulting Csörgő loops

The smallest group H that satisfies the above condition has order 64. In fact, 10 non-isomorphic groups of order 64 satisfy those properties. Moreover, there are 28 free parameters for the construction of μ. That means that in theory, we can generate as much as 10×2^{28} different loops, a little bit less than three billion. However, one should keep in mind that those loops may be isomorphic. However, experiments conducted in [5] show that the probability that two randomly chosen such loops are isomorphic is probably less than 1 / 2500. Empirically, for a loop Q generated this way, we have the following properties:

- $\mathrm{Nuc}(Q) \cong \mathbb{Z}_2^4$
- $Q \,/\, \mathrm{Nuc}(Q) \cong \mathbb{Z}_2^3$
- $Z(Q) \cong \mathbb{Z}_2$. This fact is proven in [5]
- $Q \,/\, Z(Q) \cong H$

This is as expected in the main AIM conjecture. As the authors of [5] have proved in further work, the presented method cannot yield loops of size smaller than 128. To this day, it is still an open problem to know whether or not there exist Csörgő loops of order less than 128.

6 Loop extension

This section is dedicated to showing a systematic way to generate nilpotent loops. This theoretical work will be used in the next section to try to generate small Csörgő loops. We will first introduce the notion of loop extension, and then we will see how this relates to the nilpotency class. A loop extension is a way to create a new loop from an abelian group and a loop. It can be seen as a generalization of the semi-direct product of two groups. Moreover, iterating these extensions is a theoretical way to exhaust all nilpotent loops.

6.1 Abelian and central extensions

Let $(A, +, 0)$ be an abelian group and $(Q, \cdot, 1)$ be a loop.

Definition 23. *A triplet $\Gamma = (\phi, \psi, \theta)$ is called a cocycle if*

- $\phi, \psi : Q \times Q \mapsto \mathrm{Aut}(A)$
- $\theta : Q \times Q \mapsto A$

We will note $\psi_{x,y} = \psi(x, y) \in \mathrm{Aut}(A)$ and similarly $\phi_{x,y} = \phi(x, y)$. Likewise $\theta_{x,y} = \theta(x, y) \in A$

Definition 24. *The abelian extension of A by Q over a cocycle Γ, noted $A :_\Gamma Q$, is the magma $(A \times Q, \cdot)$ where*

$$(a, x) \cdot (b, y) = (\phi_{x,y}(a) + \psi_{x,y}(b) + \theta_{x,y}, xy)$$

Under some conditions, this magma is a loop

Proposition 14. *The extension $A :_\Gamma Q$ is a loop with identity element $(0, 1)$ if and only if for every $y \in Q$*

- $\phi_{y,1} = \mathrm{Id} = \psi_{1,y}$
- $\theta_{1,y} = 0 = \theta_{y,1}$

Proof. First, we will show that $L = A :_\Gamma Q$ is a quasigroup. Indeed, setting

$$(a, x) \setminus (b, y) = (\psi^{-1}_{x,x\setminus y}(b - \phi_{x,x\setminus y}(a) - \theta_{x,x\setminus y}, x \setminus y)$$

we verify that $(a, x) \cdot ((a, x) \setminus (b, y)) = (b, y)$ because

$$\begin{aligned}
&(a, x) \cdot (\psi^{-1}_{x,x\setminus y}(b - \phi_{x,x\setminus y}(a) - \theta_{x,x\setminus y}, x \setminus y) \\
&= (\psi_{x,x\setminus y}(\psi^{-1}_{x,x\setminus y}(b - \phi_{x,x\setminus y}(a) - \theta_{x,x\setminus y}) + \psi_{x,x\setminus y}(a) + \theta_{x,x\setminus y}, x \cdot x \setminus y) \\
&= (b, y)
\end{aligned}$$

Similarly, one can prove that $(a, x) \setminus ((a, x)(b, y)) = (b, y)$. Moreover, with similar arguments, setting

$$(a, x) \,/\, (b, y) = (\phi^{-1}_{x/y,y}(a - \psi_{x/y,y}(b) - \theta_{x/y,y}), x \,/\, y)$$

we obtain a right division for the quasigroup. Note that $\psi_{x,y}(0) = 0 = \phi_{x,y}(0)$ because $\phi_{x,y}, \psi_{x,y} \in \mathrm{Aut}(A)$. Suppose $L = A :_\Gamma Q$ is a loop with identity element $(0, 1)$ then for all $y \in Q$

$$\begin{aligned}
(0, y) = (0, 1)(0, y) &\implies 0 = \phi_{1,y}(0) + \psi_{1,y}(0) + \theta_{1,y} = \theta_{1,y} \\
(0, y) = (0, y)(0, 1) &\implies 0 = \phi_{y,1}(0) + \psi_{y,1}(0) + \theta_{y,1} = \theta_{y,1}
\end{aligned}$$

so $\theta_{1,y} = 0 = \theta_{y,1}$. Now for all $y \in Q$ and for all $b \in A$

$$(b,y) = (0,1)(b,y) \implies b = \phi_{1,y}(0) + \psi_{1,y}(b) + \theta_{1,y} = \psi_{1,y}(b)$$
$$(b,y) = (b,y)(0,1) \implies b = \phi_{y,1}(b) + \psi_{y,1}(0) + \theta_{y,1} = \phi_{y,1}(b)$$

hence $\phi_{y,1} = \mathrm{Id} = \psi_{1,y}$. Conversely, the converse of the last two equalities hold whenever $\phi_{y,1} = \mathrm{Id} = \psi_{1,y}$ and $\theta_{1,y} = 0 = \theta_{y,1}$ for all $y \in Q$, meaning that L is a loop with identity $(0,1)$. □

We now refine the definition of cocycle so that the resulting extension is a loop.

Definition 25 (Cocycle)**.** *A triple $\Gamma = (\phi, \psi, \theta)$ is called a cocycle if*

- $\phi, \psi : Q \times Q \mapsto \mathrm{Aut}(A)$
- $\theta : Q \mapsto A$
- $\phi_{y,1} = \mathrm{Id} = \psi_{1,y}$
- $\theta_{1,y} = 0 = \theta_{y,1}$

Hence, the abelian extension $A :_\Gamma Q$ is a loop with identity element $(0,1)$.

Definition 26 (Central extension)**.** *An extension $A :_{(\phi,\psi,\theta)} Q$ is called a central extension if $\phi_{x,y} = \mathrm{Id} = \psi_{x,y}$ for all $x, y \in Q$. In this case, we will denote shortly $A :_{(\phi,\psi,\theta)} Q$ by $A :_\theta Q$ and we will call θ a cocycle.*

Note that in the case of central extension, we have

$$(a,x)(b,y) = (a + b + \theta_{x,y}, xy)$$

Definition 27 (Iterated central extension)**.** *A loop L is called an iterated central extension if it is either an abelian group, or it is a central extension $A :_\theta Q$ with A an abelian group and Q an iterated central extension.*

With this definition, we see that any iterated central extension is a tower of central extensions

$$L = A_n :_{\theta_n} (A_{n-1} :_{\theta_{n-1}} (\cdots :_{\theta_1} (A_1 :_{\theta_0} A_0)) \dots)$$

where A_i are $(n+1)$ abelian groups and θ_i are n cocycles. We will commonly refer as double (central) extension, the iterated central extension

$$L = A :_\theta (B :_\sigma C)$$

where A, B, C are three abelian groups and θ, σ are two cocycles. The interest of iterated central extension lies in the following theorem discussed and proved more generally in [14].

Theorem 9. *A loop is nilpotent if and only if it is an iterated central extension. Moreover, if $L = A :_\theta Q$ and $\mathrm{cl}(Q) \leq n$, then $\mathrm{cl}(L) \leq n + 1$.*

In particular, using double extensions $A :_\theta (B :_\sigma C)$ seems to be a promising way to generate loops of nilpotency class 3 with abelian inner mapping. In fact, as we will see next, this is indeed how the previous Csörgő loops were constructed. However, it is, in theory, possible that some loop of nilpotency class 3 cannot be generated merely as a double extension. Indeed in the theorem 9, nothing prevents some loops of nilpotency class 3 to be generated only by more than double extensions. However, Michael Kinyon suggested in a conversation that one could hope that all loops with nilpotency class 3 could be generated using a double extension. Hence, the rest of this thesis is dedicated to numerically and empirically study and generate such extensions in order to find smaller Csörgő loops.

6.2 Decomposition of Csörgő loops

Recall that the Csörgő loops were constructed as the product $(A \times H, \cdot)$ for H a group and $A \cong \mathbb{Z}_2$. The multiplication laws were as follow:

$$(a, x) \cdot (b, y) = (ab\mu(x, y), xy)$$

this is a central extension $A :_\mu H$. Using the LOOPS package from GAP, we can decompose further into an iterated central extension. It turns out that

$$H = \mathbb{Z}_2^3 :_\sigma \mathbb{Z}_2^3$$

for some cocycle σ. Finally, we can decompose the Csörgő loop C as the double extension

$$C = \mathbb{Z}_2 :_\mu (\mathbb{Z}_2^3 :_\sigma \mathbb{Z}_2^3)$$

In [5], it was mentioned that 10 groups H of order 64 were suitable to construct Csörgő loops using the method we described. It turns out that all those H have a decomposition $H = \mathbb{Z}_2^3 :_\sigma \mathbb{Z}_2^3$. Their id in the GAP small group library are $(64, n)$ for $73 \leq n \leq 82$. The various cocycles σthat generate them can be found in the appendix A. Hence, we can see that those Csörgő loops are constructed as an iterated central extensions with very simple elementary abelian groups. In the next section, we will try to control such iterated extension to generate smaller Csörgő loops.

7 Computational construction of iterated central extensions

Now that we have the theoretical background to lead our search for a smaller Csörgő loop, we will intensively use computational methods to explore the properties of iterated central extensions. We will see that the spaces where the loops lie are huge, and we will try to use properties of the cocycles and groups of nilpotency class three to reduce the search space. David Stanovský suggested that to construct AIM loops, one should use abelian groups of order a power of the same prime p. We will take $p \in \{2, 3\}$.

7.1 Goal and generalities

The smallest known Csörgő loops have all order $128 = 2^7$. They are all constructed by iterated extension of elementary abelian groups of order 2^k. If one wants to find a smaller Csörgő loop, it seems reasonable to search for loops of order 64 constructed in the same fashion. Thus, we would like, in theory, to compute every loop

$$L = A :_\theta (B :_\sigma C)$$

such that A, B, C are abelian groups and $|A||B||C| = 64$. Because none of the three groups should be trivial, we have

$$2 \leq |A|, |B|, |C| \leq 16$$

this leaves us with 11 different possible groups, namely

- $\mathbb{Z}_2$ for order 2
- $\mathbb{Z}_2^2$ and $\mathbb{Z}_4$ for order 4
- $\mathbb{Z}_2^3$, $\mathbb{Z}_2 \times \mathbb{Z}_4$ and $\mathbb{Z}_8$ for order 8
- $\mathbb{Z}_2^4$, $\mathbb{Z}_2^2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_8$, $\mathbb{Z}_4^2$ and $\mathbb{Z}_{16}$ for order 16

this leads to 59 different configurations that can be found in the appendix B.

Proposition 15. *If $|A| = a$ and $|B| = b$, there are $a^{(b-1)^2}$ possibilities to construct all the extensions $A :_\theta B$.*

Proof. $\theta : B \times B \mapsto A$, so for every element of $B \times B$ we have a possibilities. But remember that $\theta_{1,x}$ and $\theta_{x,1}$ are fixed so there is only $(b-1)^2$ free parameters in $B \times B$. Hence $a^{(b-1)^2}$ possibilities. □

Thus, for double extensions $A :_\theta (B :_\sigma C)$, we obtain $a^{(b^{(c-1)^2}-1)^2}$. As we can see in the appendix B, even the logarithm of this number is often too big to be exhausted numerically. Except if Csörgő loops prevail in those spaces, it is hopeless to want to generate them by shooting randomly for cocycles and extensions. We must focus our attention on very well-chosen subspaces of these vast spaces.
The loops we generate are entirely determined by the abelian groups we choose and the cocycles. Then it is interesting to know how properties of the cocycles relate to properties of loops. If this is well understood, we could use the good cocycles to create the loops we are interested in. Unfortunately, the relations between the cocycles and the resulting extension are not yet very well understood, but, for instance, cohomology techniques in the study of these cocycles in [4] allowed the authors to enumerate all nilpotent loops of order less than 24.

7.2 Simple extension $A :_\theta B$

Before studying double extensions, we can try to consider the simple central extensions $A :_\theta B$. In some particular cases, we will exhaust them all and see that the cocycles can be arranged in a lattice that creates a way to restrict our search space, in order to search for smaller Csörgő loops. Let us fix two abelian groups A and B. We would like to find a procedure, given any two cocycles θ_1, θ_2, that can tell if the resulting loops $A :_{\theta_1} B$ and $A :_{\theta_2} B$ are isomorphic. One obvious method would be to construct the extension and check for loop isomorphism. It is possible to check for isomorphism in GAP. However, this is a very time-consuming procedure, and that would give no insight on the influence of the cocycle over the resulting loop. But for instance, let us consider $A = \mathbb{Z}_2$ and $B = \mathbb{Z}_2^2$. There is $2^{(4-1)^2} = 512$ possible loop extensions $A :_\theta B$. We easily generate all the possible extensions. Then using the LOOPS package of GAP, we search for isomorphisms and we construct the set $\Theta/\sim$. We obtain 60 isomorphism classes. Among these loops, 2 of them have nilpotency class 1 and they are $\mathbb{Z}_2^3$ and $\mathbb{Z}_4 \times \mathbb{Z}_2$. We also have D_8, the quaternion group. The rest are non-associative loops of nilpotency class 2.

We are now interested in the following problem. Let $\Theta = \{\theta : B \times B \mapsto A \,|\, \forall x \in B,\ \theta_{1,x} = 0 = \theta_{x,1}\}$ the set of all cocycles for the central extension of A by B. We consider the relation $\sim$ on Θ such that:

$$\theta_1 \sim \theta_2 \text{ iff } (A :_{\theta_1} B) \cong (A :_{\theta_2} B)$$

it is straightforward to check that $\sim$ is an equivalence relation because $\cong$ is also an equivalence relation. We are naturally interested in the set $\Theta/\sim$ to understand the relationship between cocycles and loop isomorphisms. For that, we introduce a natural combination of cocycles, the cocycle addition:

Definition 28. *Let $\theta, \sigma \in \Theta$. We define the cocycle $\theta \oplus \sigma : B \times B \mapsto A$ by*

$$\forall x, y \in B,\ (\theta \oplus \sigma)_{x,y} = \theta_{x,y} + \sigma_{x,y}$$

where the $+$ is the addition law on A.

$\theta \oplus \sigma$ is also a cocycle because the boundary condition are verified given the definition. Moreover, $\oplus$ is clearly associative and commutative. The cocycle that is 0 everywhere is an identity element for $\oplus$. Hence $(\Theta, \oplus)$ is an abelian group. In fact it is isomorphic to $A^{(b-1)^2}$ where $b = |B|$ because we can see a cocycle as an element of $A^{(b-1)^2}$. Unfortunately, this law $\oplus$ does not behave correctly on the quotient set $\Theta/\sim$.

7.3 Lattice over the cocycles

7.3.1 Experimental results

To see a lattice structure over $\Theta/\sim$, let us consider a very small example where $A = B = \mathbb{Z}_3$. There are $3^4 = 81$ different loops and a total of only 10 isomorphisms classes, summarized in the table 1. We note $\Theta/\sim = \{T_0, \ldots, T_9\}$ where the index i of T_i corresponds to the Id in the table 1.

In general, the addition $\oplus$ over the cocycles is not compatible with $\sim$. Nevertheless, in certain cases it is. For instance, $(T_0, \oplus)$ is a group isomorphic to $(\mathbb{Z}_3, +)$

Id	Number of cocycles	nilp. class	$\cong$ to
0	3	1	$\mathbb{Z}_3^2$
1	12	2	
2	12	2	
3	12	2	
4	6	2	
5	12	2	
6	6	2	
7	6	2	
8	6	1	$\mathbb{Z}_9$
9	6	2	

Table 1: Structure of $\Theta/\sim$, $A = B = \mathbb{Z}_3$

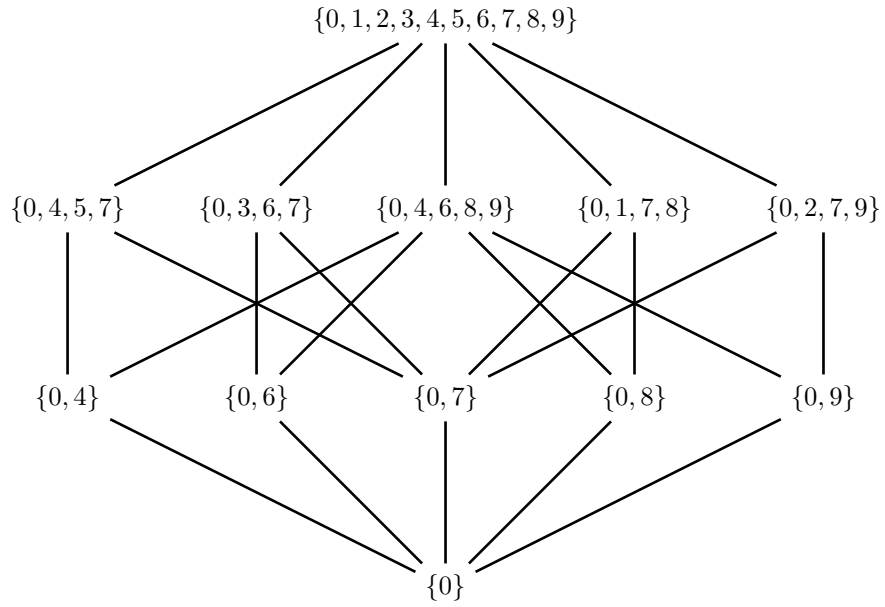

Figure 2: Lattice of subgroups from $\Theta/\sim$

with elements

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix}$$

Moreover, $(T_0 \cup T_i, \oplus)$ form a group isomorphic to $\mathbb{Z}_3^2$ for all $i \in \{4, 6, 7, 8, 9\}$, with T_0 as a subgroup. Constructing like that, we form a lattice of subgroup with T_0 at the bottom and $\bigcup_{0 \leq i \leq 9} T_i$ at the top. In this case, the lattice looks like the one in the figure 2.

In this lattice, each point $J = \{j_1, \ldots, j_k\}$ is such that

$$(\bigcup_{j \in J} T_j, \oplus)$$

is a subgroup of $\mathbb{Z}_3^r$ where r is the layer at which the point J is. For instance, the point $J = \{0, 4, 6, 8, 9\}$ is on layer 3. One can check that this lattice is modular.

Experiments on other extensions like $A = \mathbb{Z}_2$ and $B = \mathbb{Z}_2^2$ or Z_4 show similar results. To construct the lattice in the general case, we rely on the results of the next section, which have only been verified experimentally.

7.3.2 Conjectures

Let A and B be two abelian groups. Let $\Theta/\sim = \{T_0, \dots, T_{n-1}\}$ the set of n isomorphism classes. We make sure that $T_0 = [\theta_0]$ where $\theta_0 : B \times B \mapsto A$ is 0 everywhere.

Conjecture 3. *$(T_0, \oplus)$ is a group. Furthermore, for all $\theta \in T_0$*

$$A :_\theta B \cong A \times B$$

The second part of the conjecture is true because the cocycle θ_0 is in this class and $A :_{\theta_0} B$ corresponds to the classic direct product.

Definition 29. *Let $S \subseteq \Theta$. The closure of S is the smallest set $\overline{S}$ containing S that is close under $\oplus$.*

Conjecture 4. *Let $T_i \in \Theta/\sim$. There exists $i_0 = i, i_1, \dots, i_k$ such that*

$$\overline{T_i} = \bigcup_{0 \leq j \leq k} T_{i_j}$$

that is, the closure of any equivalence classes is an union of equivalence classes.

Now, if we construct some closures by induction like this:

- $L_0 = \{\overline{T} \mid T \in \Theta/\sim\}$
- $L_{n+1} = \{\overline{L \cup T} \mid (L, T) \in L_n \times \Theta/\sim\}$

then

Conjecture 5.

$$L = \bigcup_{n \in \mathbb{N}} L_n$$

is a modular sublattice of

$$\left\{ \bigcup_{i \in I} T_i \mid I \in \mathcal{P}\left(\{0, \dots, n-1\}\right) \right\}$$

with $\subseteq$. Moreover, each element of the lattice L is isomorphic to A^r for some $r > 0$.

Note that $\bigcup_{n \in \mathbb{N}} L_n$ is not really an infinite union because L_n is stationary after some time. Those results are experimentally true for some small A and B. Let us assume they are and let us try to generate Csörgő loops using the closure properties of the lattice.

7.4 Perturbation of groups of order 64

We consider the following idea to generate Csörgő loops of order 64: we gather every group of order 64 and nilpotency class 3 (there are 114 such groups). Once this is done, we decompose them as a double extension $A :_\theta (B :_\sigma C)$ and we put together the cocycles that have the same A, B and C. That is, if we say that $t(G)$ is the cocycle θ in the decomposition of G and $s(G)$ is the σ, then

$$T_{A,B,C} = \{t(G) \,|\, |G| = 64,\ \mathrm{cl}(G) = 3,\ G = A :_{t(G)} (B :_{s(G)} C)\}$$

and

$$S_{A,B,C} = \{s(G) \,|\, |G| = 64,\ \mathrm{cl}(G) = 3,\ G = A :_{t(G)} (B :_{s(G)} C)\}$$

The different A, B, C, as well as the number of groups having those as decomposition, are summarized in the table 2.

A	B	C	Number of groups
$\mathbb{Z}_2^3$	$\mathbb{Z}_2$	$\mathbb{Z}_2^2$	8
$\mathbb{Z}_4 \times \mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_2^2$	14
$\mathbb{Z}_8$	$\mathbb{Z}_2$	$\mathbb{Z}_2^2$	3
$\mathbb{Z}_2^2$	$\mathbb{Z}_2^2$	$\mathbb{Z}_2^2$	69
$\mathbb{Z}_4$	$\mathbb{Z}_2^2$	$\mathbb{Z}_2^2$	8
$\mathbb{Z}_2$	$\mathbb{Z}_2^3$	$\mathbb{Z}_2^2$	3
$\mathbb{Z}_2$	$\mathbb{Z}_2^2$	$\mathbb{Z}_2^3$	9

Table 2: Classification of the 114 groups of nilpotency 3 and order 64

We now fix A, B and C (such that the triplet appears in the table 2) and we extend $T_{A,B,C}$ and $S_{A,B,C}$ by taking their closure under $\oplus$ that are $\overline{T_{A,B,C}}$, and $\overline{S_{A,B,C}}$. Finally, we compute all the extensions:

$$\mathcal{L} = \left\{A :_\theta (B :_\sigma C) \,|\, (\theta, \sigma) \in \overline{T_{A,B,C}} \times \overline{S_{A,B,C}}\right\}$$

The hope is that in $\mathcal{L}$ there will be loops close enough to groups of nilpotency class 3 with abelian inner mapping. This hope comes from the fact that the loops constructed in [5] are loops that are somehow close to groups. They were constructed by modifications of groups. This experiment proposes to do the same thing, starting from groups and extending them to loops, respecting a certain closeness concerning the cocycle that comes from the lattice structure described previously. Unfortunately, no Csörgő loops were found by this method. However, loops close to be Csörgő were found. Indeed, some loops L generated by this method were not associative, had nilpotency class 3, and were such that $|\operatorname{Inn}(L)'| = 2$. That is, loops whose inner mapping group was very close to being abelian in the sense that the commutator subgroup has only size 2. Moreover, this method allows to generate quickly many loops of nilpotency class 3 with relatively small inner mapping groups, that can be of interest.

8 Conclusion

The first goal of this thesis was to give an understanding of the AIM conjecture and the importance of Csörgő loops. In this regard, we hope it was successful, even for someone who has never studied loop theory. The second goal was to try to exhibit Csörgő loops of smaller size. Csörgő loops are a very specific type of loops, and finding them among the vast possibilities of loops of nilpotency class 3 will probably require more than naive computer search. That is what we tried to do in this thesis. The double central extension seemed a good way to find them, and additional work could lead to interesting results, especially using the cocycle modification from groups of nilpotency class 3 and order 64. In order to find Csörgő loops, more precise search algorithms will be required, and well-tuned metrics to quantify how close a loop is to be Csörgő is needed. Indeed, in this thesis, the only metric we use to quantify "how AIM a loop is", is the size of the derived subgroup on the inner mapping group. Although this metric is theoretically appropriate, it does not seem to respect the symmetries of our problem. One would want to study further the influences of the cocycles and extensions. For instance, instead of the relation $\sim$ that clusters the cocycles with respect to isomorphisms of the resulting loops, one could imagine using looser equivalence relation $\sim'$ that classified loops with respect to some other invariant, like a set of axioms relevant to the AIM problem. Indeed, in [9], we see that being AIM can be stated in first-order logic, and we can imagine a set of larger properties where $\Theta/\sim'$ *respects* the AIM and the nilpotency.

One last problem is that we are maybe searching for something that does not exist. Nothing guarantees that smaller Csörgő loops exist. Maybe the smallest examples are of size 128, and thus, all our efforts are hopeless. However, to prove such a statement would require mathematical insight.

A Decomposition of H

In the table 4, one can found the different cocycles used in the decomposition of the ten groups $H = \mathbb{Z}_2^3 :_\sigma \mathbb{Z}_2^3$ that are suitable for constructing the Csörgő loops with the method described in [5]. The caption of each table represents the id of the group in the small group library of GAP. Note that those numbers are highly dependent on a chosen representation of $\mathbb{Z}_2^3$. Here we choose the one in table 3.

Table 3: A multiplication table of $\mathbb{Z}_2^3$

	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	4	5	2	3	7	6
2	2	4	0	6	1	7	3	5
3	3	5	6	0	7	1	2	4
4	4	2	1	7	0	6	5	3
5	5	3	7	1	6	0	4	2
6	6	7	3	2	5	4	0	1
7	7	6	5	4	3	2	1	0

Table 4: Cocycle σ for constructing H

Table 5: (64, 73)

0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	1	0	0	1	1	0	1
0	2	3	0	6	2	3	6
0	1	0	0	1	1	0	1
0	2	3	0	6	2	3	6
0	4	3	0	7	4	3	7
0	4	3	0	7	4	3	7

Table 6: (64, 74)

0	0	0	0	0	0	0	0
0	1	0	0	1	1	0	1
0	1	1	0	0	1	1	0
0	2	3	0	6	2	3	6
0	0	1	0	1	0	1	1
0	4	3	0	7	4	3	7
0	4	5	0	6	4	5	6
0	2	5	0	7	2	5	7

Table 7: (64, 75)

0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	1	0	0	1	1	0	1
0	2	3	1	6	4	5	7
0	1	0	0	1	1	0	1
0	2	3	1	6	4	5	7
0	4	3	1	7	2	5	6
0	4	3	1	7	2	5	6

Table 8: (64, 76)

0	0	0	0	0	0	0	0
0	1	0	0	1	1	0	1
0	1	1	0	0	1	1	0
0	2	3	1	6	4	5	7
0	0	1	0	1	0	1	1
0	4	3	1	7	2	5	6
0	4	5	1	6	2	3	7
0	2	5	1	7	4	3	6

Table 9: (64, 77)

0	0	0	0	0	0	0	0
0	4	0	0	4	4	0	4
0	1	1	0	0	1	1	0
0	2	3	0	6	2	3	6
0	2	1	0	4	2	1	4
0	1	3	0	5	1	3	5
0	4	5	0	6	4	5	6
0	0	5	0	5	0	5	5

Table 10: (64, 78)

0	0	0	0	0	0	0	0
0	2	0	0	2	2	0	2
0	1	0	0	1	1	0	1
0	2	3	1	6	4	5	7
0	4	0	0	4	4	0	4
0	0	3	1	3	1	5	5
0	4	3	1	7	2	5	6
0	1	3	1	5	0	5	3

Table 11: (64, 79)

0	0	0	0	0	0	0	0
0	2	0	0	2	2	0	2
0	1	1	0	0	1	1	0
0	2	3	1	6	4	5	7
0	4	1	0	2	4	1	2
0	0	3	1	3	1	5	5
0	4	5	1	6	2	3	7
0	1	5	1	3	0	3	5

Table 12: (64, 80)

0	0	0	0	0	0	0	0
0	1	0	0	1	1	0	1
0	1	4	0	2	1	4	2
0	2	3	0	6	2	3	6
0	0	4	0	4	0	4	4
0	4	3	0	7	4	3	7
0	4	7	0	3	4	7	3
0	2	7	0	5	2	7	5

Table 13: (64, 81)

0	0	0	0	0	0	0	0
0	1	0	0	1	1	0	1
0	1	4	0	2	1	4	2
0	2	3	1	6	4	5	7
0	0	4	0	4	0	4	4
0	4	3	1	7	2	5	6
0	4	7	1	3	2	6	5
0	2	7	1	5	4	6	3

Table 14: (64, 82)

0	0	0	0	0	0	0	0
0	7	0	0	7	7	0	7
0	1	4	0	2	1	4	2
0	2	3	1	6	4	5	7
0	6	4	0	5	6	4	5
0	5	3	1	1	3	5	0
0	4	7	1	3	2	6	5
0	3	7	1	4	5	6	2

B All double extensions of order 64

In the table 15, we list all the possible double extensions that lead to loops of order 64. The last column indicates n, such that 2^n is the number of different cocycles θ, σ that can be used to generate $A :_\theta (B :_\sigma C)$. Note that two different cocycles can lead to isomorphic loops.

A	B	C	$\log_2$ number of cocycles
$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_2^4$	5.392×10^{67}
$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_2^2 \times \mathbb{Z}_4$	5.392×10^{67}
$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_8$	5.392×10^{67}
$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_4^2$	5.392×10^{67}
$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_{16}$	5.392×10^{67}
$\mathbb{Z}_2$	$\mathbb{Z}_2^2$	$\mathbb{Z}_2^3$	3.169×10^{29}

$\mathbb{Z}_2$	$\mathbb{Z}_2^2$	$\mathbb{Z}_2 \times \mathbb{Z}_4$	3.169×10^{29}
$\mathbb{Z}_2$	$\mathbb{Z}_2^2$	$\mathbb{Z}_8$	3.169×10^{29}
$\mathbb{Z}_2$	$\mathbb{Z}_4$	$\mathbb{Z}_2^3$	3.169×10^{29}
$\mathbb{Z}_2$	$\mathbb{Z}_4$	$\mathbb{Z}_2 \times \mathbb{Z}_4$	3.169×10^{29}
$\mathbb{Z}_2$	$\mathbb{Z}_4$	$\mathbb{Z}_8$	3.169×10^{29}
$\mathbb{Z}_2$	$\mathbb{Z}_2^3$	$\mathbb{Z}_2^2$	1.342×10^{08}
$\mathbb{Z}_2$	$\mathbb{Z}_2^3$	$\mathbb{Z}_4$	1.342×10^{08}
$\mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\mathbb{Z}_2^2$	1.342×10^{08}
$\mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\mathbb{Z}_4$	1.342×10^{08}
$\mathbb{Z}_2$	$\mathbb{Z}_8$	$\mathbb{Z}_2^2$	1.342×10^{08}
$\mathbb{Z}_2$	$\mathbb{Z}_8$	$\mathbb{Z}_4$	1.342×10^{08}
$\mathbb{Z}_2$	$\mathbb{Z}_2^4$	$\mathbb{Z}_2$	16
$\mathbb{Z}_2$	$\mathbb{Z}_2^2 \times \mathbb{Z}_4$	$\mathbb{Z}_2$	16
$\mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_8$	$\mathbb{Z}_2$	16
$\mathbb{Z}_2$	$\mathbb{Z}_4^2$	$\mathbb{Z}_2$	16
$\mathbb{Z}_2$	$\mathbb{Z}_{16}$	$\mathbb{Z}_2$	16
$\mathbb{Z}_2^2$	$\mathbb{Z}_2$	$\mathbb{Z}_2^3$	1.126×10^{15}
$\mathbb{Z}_2^2$	$\mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_4$	1.126×10^{15}
$\mathbb{Z}_2^2$	$\mathbb{Z}_2$	$\mathbb{Z}_8$	1.126×10^{15}
$\mathbb{Z}_2^2$	$\mathbb{Z}_2^2$	$\mathbb{Z}_2^2$	524288
$\mathbb{Z}_2^2$	$\mathbb{Z}_2^2$	$\mathbb{Z}_4$	524288
$\mathbb{Z}_2^2$	$\mathbb{Z}_4$	$\mathbb{Z}_2^2$	524288
$\mathbb{Z}_2^2$	$\mathbb{Z}_4$	$\mathbb{Z}_4$	524288
$\mathbb{Z}_2^2$	$\mathbb{Z}_2^3$	$\mathbb{Z}_2$	16
$\mathbb{Z}_2^2$	$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\mathbb{Z}_2$	16
$\mathbb{Z}_2^2$	$\mathbb{Z}_8$	$\mathbb{Z}_2$	16
$\mathbb{Z}_4$	$\mathbb{Z}_2$	$\mathbb{Z}_2^3$	1.126×10^{15}
$\mathbb{Z}_4$	$\mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_4$	1.126×10^{15}
$\mathbb{Z}_4$	$\mathbb{Z}_2$	$\mathbb{Z}_8$	1.126×10^{15}
$\mathbb{Z}_4$	$\mathbb{Z}_2^2$	$\mathbb{Z}_2^2$	524288
$\mathbb{Z}_4$	$\mathbb{Z}_2^2$	$\mathbb{Z}_4$	524288
$\mathbb{Z}_4$	$\mathbb{Z}_4$	$\mathbb{Z}_2^2$	524288
$\mathbb{Z}_4$	$\mathbb{Z}_4$	$\mathbb{Z}_4$	524288

$\mathbb{Z}_4$	$\mathbb{Z}_2^3$	$\mathbb{Z}_2$	16
$\mathbb{Z}_4$	$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\mathbb{Z}_2$	16
$\mathbb{Z}_4$	$\mathbb{Z}_8$	$\mathbb{Z}_2$	16
$\mathbb{Z}_2^3$	$\mathbb{Z}_2$	$\mathbb{Z}_2^2$	1536
$\mathbb{Z}_2^3$	$\mathbb{Z}_2$	$\mathbb{Z}_4$	1536
$\mathbb{Z}_2^3$	$\mathbb{Z}_2^2$	$\mathbb{Z}_2$	12
$\mathbb{Z}_2^3$	$\mathbb{Z}_4$	$\mathbb{Z}_2$	12
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\mathbb{Z}_2$	$\mathbb{Z}_2^2$	1536
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\mathbb{Z}_2$	$\mathbb{Z}_4$	1536
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\mathbb{Z}_2^2$	$\mathbb{Z}_2$	12
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\mathbb{Z}_4$	$\mathbb{Z}_2$	12
$\mathbb{Z}_8$	$\mathbb{Z}_2$	$\mathbb{Z}_2^2$	1536
$\mathbb{Z}_8$	$\mathbb{Z}_2$	$\mathbb{Z}_4$	1536
$\mathbb{Z}_8$	$\mathbb{Z}_2^2$	$\mathbb{Z}_2$	12
$\mathbb{Z}_8$	$\mathbb{Z}_4$	$\mathbb{Z}_2$	12
$\mathbb{Z}_2^4$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	8
$\mathbb{Z}_2^2 \times \mathbb{Z}_4$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	8
$\mathbb{Z}_2 \times \mathbb{Z}_8$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	8
$\mathbb{Z}_4^2$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	8
$\mathbb{Z}_{16}$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	8

Table 15: List of all double extension leading to loops of order 64

References

[1] R. H. Bruck. "Contributions to the theory of loops". In: *Transactions of the American Mathematical Society* 60 (1946), pp. 245–245. DOI: 10.1090/s0002-9947-1946-0017288-3. URL: https://doi.org/10.1090/s0002-9947-1946-0017288-3.

[2] Anthony E. Clement, Stephen Majewicz, and Marcos Zyman. "Introduction to Nilpotent Groups". In: *The Theory of Nilpotent Groups*. Cham: Springer International Publishing, 2017, pp. 23–73. ISBN: 978-3-319-66213-8. DOI: 10.1007/978-3-319-66213-8_2. URL: https://doi.org/10.1007/978-3-319-66213-8_2.

[3] Piroska Csörgő. "Abelian inner mappings and nilpotency class greater than two". In: *European Journal of Combinatorics* 28.3 (2007), pp. 858–867. ISSN: 0195-6698. DOI: https://doi.org/10.1016/j.ejc.2005.12.002.

[4] Daniel Daly and Petr Vojtěchovský. *Enumeration of nilpotent loops via cohomology*. 2015. arXiv: 1509.05713 [math.GR].

[5] Aleš Drápal and Petr Vojtěchovský. *Explicit constructions of loops with commuting inner mappings*. 2015. arXiv: 1509.05706 [math.GR].

[6] *GAP – Groups, Algorithms, and Programming, Version 4.11.1*. The GAP Group. 2021. URL: https://www.gap-system.org.

[7] T. Kepka and J. Phillips. "Connected transversals to subnormal subgroups". In: 1997.

[8] Michael Kinyon. *Loops And The AIM Conjecture*. Department of Mathematics, University of Denver. July 13, 2016.

[9] Michael Kinyon, Robert Veroff, and Petr Vojtěchovský. "Loops with abelian inner mapping groups: An application of automated deduction". In: *arXiv e-prints*, arXiv:1509.05468 (Sept. 2015), arXiv:1509.05468. arXiv: 1509.05468 [math.GR].

[10] Gábor P. Nagy and Petr Vojtěchovský. *Moufang loops with commuting inner mappings*. 2015. arXiv: 1509.05709 [math.GR].

[11] Markku Niemenmaa and Tomas Kepka. "On connected transversals to Abelian subgroups". In: *Bulletin of the Australian Mathematical Society* 49 (Feb. 1994), pp. 121–128. DOI: 10.1017/S0004972700016166.

[12] H.O. Pflugfelder. *Quasigroups and Loops: Introduction*. Sigma series in pure mathematics. Heldermann, 1990. ISBN: 9783885380078. URL: https://books.google.cz/books?id=MQbvAAAAMAAJ.

[13] J. Phillips and Petr Vojtěchovský. "The varieties of loops of Bol-Moufang type". In: *Algebra universalis* 54 (Feb. 2007). DOI: 10.1007/s00012-005-1941-1.

[14] David Stanovský and Petr Vojtěchovský. *Abelian extensions and solvable loops*. 2015. arXiv: 1509.05733 [math.GR].