2022

On Loop Commutators, Quaternionic Automorphic Loops, and Related Topics

Mariah Kathleen Barnes
University of Denver

On Loop Commutators, Quaternionic Automorphic Loops, and Related Topics

---

A Dissertation

Presented to

the Faculty of the College of Natural Sciences and Mathematics

University of Denver

In Partial Fulfillment

of the Requirements for the Degree

Doctor of Philosophy

---

by

Mariah Kathleen Barnes

June 2022

Advisor: Dr. Michael Kinyon

Author: Mariah Kathleen Barnes
Title: On Loop Commutators, Quaternionic Automorphic Loops, and Related Topics
Advisor: Dr. Michael Kinyon
Degree Date: June 2022

ABSTRACT

This dissertation deals with three topics inside loop and quasigroup theory. First, as a continuation of the project started by David Stanovský and Petr Vojtěchovský, we study the commutator of congruences defined by Freese and McKenzie in order to create a more pleasing, equivalent definition of the commutator inside of loops. Moreover, we show that the commutator can be characterized by the generators of the inner mapping group of the loop. We then translate these results to characterize the commutator of two normal subloops of any loop.

Second, we study automorphic loops with the desire to find more examples of small orders. Here we construct a family of automorphic loops, called quaternionic automorphic loops, which have order 2^n for $n \geq 3$, and prove several theorems about their structure. Although quaternionic automorphic loops are nonassociative, many of their properties are reminiscent of the generalized quaternion groups.

Lastly, we find varieties of quasigroups which are isotopic to commutative Moufang loops and prove their full characterization. Moreover, we define a new variety of quasigroups motivated by the semimedial quasigroups and show that they have an affine representation over commutative Moufang loops similar to the semimedial case proven by Kepka.

ACKNOWLEDGEMENTS

This dissertation is dedicated to my husband, *el amor de mi vida*, Conancio – who has sacrificed so much for me and this dream of mine.

While this acknowledgment does not do my gratitude justice, I would like to thank first and foremost my advisor Michael Kinyon. His patience, encouragement, enthusiasm, and true talent for both teaching and mathematics are the reasons why I have come so far in these last few years. From him I have learned how to grow as a mathematician and as a teacher.

I would also like to thank Petr Vojtěchovský for his contributions to my education in the field, and also his support throughout my time at the University of Denver. As the other members of my committee, I want to thank Andrew Linshaw and Matt Rutherford for their commitment to me and this dissertation. In addition, I would like to thank in a particular way Professor Natasha Dobrinen. I would not be here today without her support and encouragement.

Finally, my support system outside of the University – my family – deserves a very special thanks. I would name them all but there are simply too many of us now, so to my mother Eileen I say this: Everything I am I owe to you. Thank you for being my best cheerleader in life, and thank you for giving me my sister Tara to pick up where you left off. To my father Richard: You are such an inspiration to me, a muse of grit, showing me that life is what you make of it and you can always give more than you receive.

TABLE OF CONTENTS

Chapter 1: Introduction

Much of loop theory owes its development to the efforts to try to generalize group theory, and as such, loops are often viewed through the lens of a “nonassociative group.” While it is useful and enlightening to generalize groups by removing associativity, in many cases this process makes calculations more convoluted and difficult. Thus, it is also a project of loop theory to find structures which are, in a sense, “well-behaved” like groups without making use of the full power of associativity. One example is the variety of automorphic loops, whose inner mappings are all automorphisms (as they are in the group case, but not always in the nonassociative case). A working theory of automorphic loops has been laid down by Kinyon, Phillips, Vojtěchovský, and others in [28, 19], but there are relatively few concrete examples of small orders. Thus, one of the goals of this dissertation is to construct a family of automorphic loops of order 2^n for any $n \geq 3$ and to prove some basic facts about their structure, which is reminiscent of the structure of the generalized quaternion groups.

Another variety of loops which is “close to” groups is the variety of commutative Moufang loops (CMLs). Since CMLs have been well studied, it is useful to be able to represent certain nonassociative structures which are not as well understood – such as certain varieties quasigroups – as isotopic (a generalization of isomorphic) to CMLs. Thus, another goal of this dissertation is to give a complete representation theorem of such a variety of quasigroups. Moreover, we present a new variety of quasigroups which we call *semiparamedial*, which turn out to have an affine representation over CMLs.

Lastly, like groups, loops form a variety, and thus can also be viewed through the lens of universal algebra. From this standpoint, a loop can be defined as an algebra $(Q, \cdot, \backslash, /, 1)$ satisfying certain identities. Many times in loop theory the group-theoretical approach aligns with the universal-algebraic approach. However, one important area where they differ is in solvability. Defining solvability in loops by mimicking the group theory definition ends up not coinciding with the definition brought about from using the notion of congruence solvability from universal algebra. It remains an open question in which varieties of loops the two notions of solvability coincide, and where they differ. It is our belief that one part of why this question has gone unanswered is that there has not been a workable definition of what the commutator of two subloops is. Thus, our last goal in this manuscript is to build on the work of Stanovský and Vojtěchovský in [40] and create a more pleasing, and perhaps more useful, definition of the loop commutator.

1.1 Structure of the dissertation

Chapter 2 gives a basic introduction to loop and quasigroup theory, important definitions, and well-known results. Following this background, the dissertation is divided into three main sections. The goal of chapter 3 is to present a new definition of the loop commutator. Thus, in this chapter, we go through a brief history of the loop commutator, discuss briefly the problem of solvability, and describe the progress made by Stanovský and Vojtěchovský to write the commutator in terms of generators. In Section 3.4 we present our new definition of the loop commutator and prove that it is equivalent to the previous definitions. This new representation of the loop commutator then allows us to answer an open question presented by Stanovský and Vojtěchovský in [41].

In chapter 4, we present a construction of a family of automorphic loops which we define as *quaternionic automorphic loops*. Just as the generalized quaternion groups can be constructed in a similar way to the dihedral groups, the construction of quaternionic automorphic loops is inspired by the construction of the dihedral-like automorphic loops done by Aboras in [1]. We then prove several theorems about these loops, some of which are reminiscent of their quaternion group analogs.

Chapter 5 is dedicated to developing a representation theorem for quasigroups which are isotopic to commutative Moufang loops. Thus, we give a brief introduction to CMLs, some previous results in the field, and finally prove the full characterization. Moreover, we define "semiparamedial" quasigroups and show they have an affine representation over CMLs.

The appendix includes some GAP code which was used during the course of this investigation.

Chapter 2: Background

Here we lay out basic definitions in loop and quasigroup theory, as well as some basics of universal algebra. Moreover, we give some notation conventions and important results in the field. For an extensive study of the theories, and as a secondary reference for what follows, we direct the reader to [2, 6, 8, 33, 38].

As mentioned in the introduction, the study of loop and quasigroup theory owes much of its progress to the efforts to generalize group theory. Thus, it is common to define a *quasigroup* as a set with a binary operation, $(Q, \cdot)$ such that for every $a, b \in Q$ there exist unique $x, y \in Q$ such that $a \cdot x = b$ and $y \cdot a = b$. This is commonly known in group theory as *unique solvability*. Then a *loop* is a quasigroup with a necessarily unique identity element 1 such that $1 \cdot x = x \cdot 1 = x$ for every $x \in Q$.

Since loops and quasigroups have unique solvability, their multiplication tables form a Latin square, but more importantly, the left and right translation maps defined as follows are permutations on Q:

$$L_x : Q \to Q \quad L_x(a) = x \cdot a, \qquad \text{and} \qquad R_x : Q \to Q \quad R_x(a) = a \cdot x\,.$$

Thus, we may define new operations on Q using their inverse maps. That is, the inverse permutations L_x^{-1} and R_x^{-1} yield division operations $\backslash$ and $/$, defined by $L_x^{-1}(a) = x\backslash a$ and $R_x^{-1}(a) = a/x$.

The reason that loops and quasigroups are often thought of as "non-associative" groups comes from the fact that a quasigroup Q with the property that $x \cdot yz = xy \cdot z$ is, in fact, a group. That is, an associative quasigroup has unique two-sided inverses and a unique two-sided identity element. This is a straightforward exercise.

Loop theory and quasigroup theory also have roots in universal algebra, so we present here only a few of the necessary definitions to understand these structures through this lens. We will only be dealing here with finitary universal algebras, or universal algebras where the set I below is finite.

Definition 2.1. A *universal algebra* is a tuple $\mathbf{A} = (A, \{f_i\}_{i\in I})$ where A and I are sets and each f_i is an operation on A.

The *signature* of a universal algebra $\mathbf{A} = (A, \{f_i\}_{i\in I})$ is an $|I|$-tuple where the i^{th} entry is the arity of f_i.

We note that the following is not the standard definition of a variety, but will suffice for our purposes.

Definition 2.2. A *variety* is the class of all universal algebras of a given signature satisfying a given set of identities.

Since varieties are defined equationally, they are closed under taking appropriate quotients, sub-varieties, products and homomorphic images.

With this in mind, we may equivalently define *quasigroups* as a variety of universal algebras $(Q, \cdot, \backslash, /)$ with signature $(2, 2, 2)$ satisfying:

$$x \cdot (x\backslash y) = y\,, \quad x\backslash(x \cdot y) = y\,, \quad (x/y) \cdot y = x\,, \quad (x \cdot y)/y = x\,.$$

Then *loops* are a variety of universal algebras $(Q, \cdot, \backslash, /, 1)$ with signature $(2, 2, 2, 0)$ satisfying:

$$1 \cdot x = x\,, \quad x \cdot 1 = x\,, \quad x \cdot (x\backslash y) = y\,, \quad x\backslash(x \cdot y) = y\,, \quad (x/y) \cdot y = x\,, \quad (x \cdot y)/y = x\,.$$

It is a straightforward calculation to show that the two definitions of loops (and alternatively of quasigroups) are equivalent. Thus, we will employ either definition throughout the course of this dissertation.

To simplify notation, we will follow convention and use juxtaposition in place of $\cdot$, where juxtaposition is more binding than $\cdot, \backslash$, and $/$. In addition, $\cdot$, when used explicitly, will be less binding than $/$ or $\backslash$. For example, $xy/z = (x \cdot y)/z$, $xy \cdot z = (x \cdot y) \cdot z$, and $x \cdot y/z = x \cdot (y/z)$.

2.1 Substructures

As one might imagine, a *subquasigroup* of a quasigroup Q is a nonempty subset of Q which is closed under $\cdot, /, \backslash$, and a *subloop* is defined similarly. We denote subquasigroups and subloops as $H \leq Q$.

In the context of loops, we may define normal subloops in a way which mimics the classic group theory definition.

Definition 2.3. Let Q be a loop and $H \leq Q$. Then H is normal in Q if and only if for every $x, y \in Q$,

$$xH = Hx\,, \qquad (xH)y = x(Hy)\,, \qquad \text{and} \qquad x(yH) = (xy)H\,.$$

Since we are not guaranteed that every subloop of a loop has a coset decomposition which partitions the loop, we define the following.

Definition 2.4. Let Q be a loop and $H \leq Q$. Then saying Q has a *left (right) coset decomposition modulo* H means that the set of all left (right) cosets modulo H is a partition of Q.

We use the notation $H \trianglelefteq Q$ or $H \triangleleft Q$ to denote when H is normal in Q. For a loop Q and $H \trianglelefteq Q$, we may take Q modulo H in the usual way to form the *quotient loop*, $Q/H = \{xH\ : x \in Q\}$.

Just as is the case in group theory, loops (or quasigroups) have special subloops (or subquasigroups) which play important roles in their structure. We define these here in the context of quasigroups, noting that loops are simply a special variety of quasigroups, so the definitions apply to loops as well.

Definition 2.5. Let Q be a quasigroup. Then the *left nucleus of* Q is

$$N_\lambda(Q) = \{x \in Q : x(yz) = (xy)z \quad \forall y, z \in Q\} ,$$

the *middle nucleus of* Q is

$$N_\mu(Q) = \{y \in Q : x(yz) = (xy)z \quad \forall x, z \in Q\} ,$$

and the *right nucleus of* Q is

$$N_\rho(Q) = \{z \in Q : x(yz) = (xy)z \quad \forall x, y \in Q\} .$$

Then the full nucleus, or simply just the *nucleus of* Q is

$$N(Q) = N_\lambda(Q) \cap N_\mu(Q) \cap N_\rho(Q) .$$

In other words, the nucleus of a quasigroup is the set of all elements which associate with every element in the quasigroup.

Definition 2.6. Let Q be a quasigroup. Then the *commutant of* Q is

$$C(Q) = \{x \in Q : xy = yx \quad \forall y \in Q\} ,$$

and the *center of Q* is

$$Z(Q) = C(Q) \cap N(Q)\,.$$

Hence, the center of a quasigroup is the set of all elements which both associate and commute with all elements of the quasigroup.

We note that for any given quasigroup Q, there is no guarantee that the nuclei or the center are nonempty. However, if any of the nuclei or the center is nonempty, then it will form a subquasigroup of Q. To show, for example, that a nonempty $N_\lambda(Q)$ is closed under $\cdot$, we let $x, y \in N_\lambda(Q)$ and $a, b \in Q$. Then $xy \cdot ab = x(y \cdot ab)$ since $x \in N_\lambda$, and $x(y \cdot ab) = x(ya \cdot b)$ since $y \in N_\lambda$, and $x(ya \cdot b) = (x \cdot ya)b = (xy \cdot a)b$ since $x \in N_\lambda$. Thus, $xy \in N_\lambda(Q)$. If Q is a loop, then it is straightforward to show that the identity element is in each of $N(Q)$ and $Z(Q)$. In addition, we have the following.

Proposition 2.1. For a loop Q, the center of Q is normal in Q. Moreover, any subloop of $Z(Q)$ is normal in Q.

2.2 Mapping Groups

As stated in the definition of a quasigroup, the left and right translation maps of a quasigroup Q are permutations on Q. These generate the permutation group defined as follows.

Definition 2.7. The *multiplication group of a quasigroup Q* is

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

For loops in particular, we may define the *inner mapping group of Q* as the stabilizer of 1 in the multiplication group. It is well known (for proof, see [33]) that the inner mapping group of a loop is generated by

$$\mathrm{Inn}(Q) = \langle T_x \, , L_{x,y} \, , R_{x,y} \; : x, y \in Q \rangle \, ,$$

where

$$T_x = R_x^{-1} L_x \, , \qquad R_{x,y} = R_{yx}^{-1} R_x R_y \, , \qquad L_{x,y} = L_{xy}^{-1} L_x L_y \, .$$

Notice that the map T_x is, in a sense, a measure of commutativity, similar to the conjugation map from group theory. Moreover, the maps $L_{x,y}$ and $R_{x,y}$ are measures of associativity, and thus have no analogs in the associative setting.

It can be useful to consider the subgroups of $\mathrm{Inn}(Q)$ generated by each of these maps separately. Thus,

Definition 2.8. The *left inner mapping group of a loop Q* is

$$\mathrm{LInn}(Q) = \langle L_{x,y} : x, y \in Q \rangle.$$

The *right inner mapping group of a loop Q* is

$$\mathrm{RInn}(Q) = \langle R_{x,y} : x, y \in Q \rangle.$$

And the *middle inner mapping group of a loop Q* is

$$\mathrm{MInn}(Q) = \langle T_x : x \in Q \rangle.$$

2.3 Homomorphisms and Isomorphisms

In addition to maps on the quasigroup itself, we may define maps from one quasigroup to another. The classic definition of homomorphism and isomorphism applies, formally stated as follows.

Definition 2.9. Let $(Q, \cdot)$ and $(S, *)$ be quasigroups. Then a map $\varphi : Q \to S$ is a *homomorphism of quasigroups* if, for every $x, y \in Q$, $\varphi(x \cdot y) = \varphi(x) * \varphi(y)$. We say φ is an *isomorphism of quasigroups* if φ is a bijection. In the case when $(Q, \cdot) = (S, *)$ and φ is an isomorphism, we say φ is an *automorphism of* Q.

Definition 2.10. The set of all automorphisms of a quasigroup Q is called the *automorphism group of* Q, denoted $\mathrm{Aut}(Q)$.

In the case when Q and S are loops, we define the kernel of a homomorphism as expected.

Definition 2.11. Given a homomorphism of loops $\varphi : Q \to S$, the *kernel* of φ is the set of all elements of Q which map to the identity element in S. That is,

$$\ker \varphi = \{a \in Q : \varphi(a) = 1_S\}.$$

Just as in the group case, the kernel of a homomorphism is a normal subloop of the loop, and we get isomorphism theorems similar to those in group theory. For a proof of the Fundamental Homomorphism Theorem, see [6], and then the others follow similarly.

2.4 More on Normality

Many times working with the multiplication group or the inner mapping group of a loop can make for simpler calculations. Thus, we have the following equivalent definition of normality. For a proof of the equivalence, see [33].

Proposition 2.2. Let Q be a loop and $H \leq Q$. Then H *is normal in* Q if and only if for every $\varphi \in \mathrm{Inn}(Q)$, $\varphi(H) = H$.

Looking at the fixed points of the three generators of the inner mapping group tells more than just normality. As stated previously, T_x measures commutativity. Thus, it is straightforward to see that for some q in a quasigroup Q, $T_x(q) = q$ for all $x \in Q$ if and only if $q \in C(Q)$. Moreover, $L_{x,y}$ and $R_{x,y}$ measure associativity. So, for some $q \in Q$, $L_{x,y}(q) = q$ for all $x, y \in Q$ if and only if $q \in N_\rho(Q)$. Similarly, $R_{x,y}(q) = q$ for all $x, y \in Q$ if and only if $q \in N_\lambda(Q)$.

While it can be the case that the cosets of a subloop do not partition the loop, we do have that the cosets of normal subloops partition the loop, as definition 2.3 suggests. Thus, the index of a normal subloop in a finite loop makes sense to define. In fact, for a finite loop Q, it is enough for Q to have a left and right coset decomposition modulo a subloop H to define the index as follows.

Definition 2.12. Let Q be a finite loop and $H \leq Q$ such that Q has a left and right coset decomposition modulo H. The *index of* H *in* Q, denoted $[Q : H]$, is the number of cosets of H in Q.

It is not difficult to see that if $[Q : H]$ makes sense then $[Q : H] = \frac{|Q|}{|H|}$. It also holds that if $[Q : H] = 2$, then $H \lhd Q$, using the same proof as the group case.

2.5 Isotopisms

Another type of mapping between quasigroups is called an *isotopism*. These are generalizations of the notion of an isomorphism, and are useful in many settings in nonassociative algebra.

Definition 2.13. Let $(Q, \cdot)$ and $(S, \circ)$ be quasigroups. An *isotopism* from $(Q, \cdot)$ to $(S, \circ)$ is a triple of bijections (α, β, γ) from Q to S such that for every $x, y \in Q$,

$$\alpha(x) \circ \beta(y) = \gamma(x \cdot y).$$

Then Q and S are said to be *isotopic*, or that S is an *isotope* of Q.

In the case where $(Q, \cdot) = (S, \circ)$, then (α, β, γ) is an *autotopism*.

In the case where $Q = S$ and $\gamma = \mathrm{id}$, then $(\alpha, \beta, \mathrm{id}) : (Q, \cdot) \to (Q, \circ)$ is a *principle isotopism*.

It is fairly clear to see that isotopy is a generalization of isomorphy. Take, for instance, the isotopism $(\varphi,\varphi,\varphi):(Q,\cdot)\to(S,\circ)$. This means simply, for every $x,y\in Q$, $\varphi(x)\circ\varphi(y)=\varphi(x\cdot y)$, which is precisely the definition of isomorphism.

It is useful on many occasions to study the isotopes of a loop or quasigroup. To do so, it is sufficient to study just the principle isotopes, as the following theorem suggests. For a proof, see [33].

Theorem 2.3. If $(Q,\cdot)$ and $(S,\circ)$ are isotopic quasigroups, then $(S,\circ)$ is isomorphic to some principle isotope of $(Q,\cdot)$.

2.6 Special Types of Loops and Quasigroups

As implied in Chapter 1, there are several varieties of loops and quasigroups which receive special attention because they have nice properties or are similar to groups in some way. We introduce here only two of the varieties which will appear in this dissertation, the rest will be defined as needed throughout the course of this study.

Those familiar with group theory may recall a structure similar to $\mathrm{Inn}(Q)$ called the inner automorphism group. However, once associativity is no longer assumed, it is not necessary that the inner mappings of a loop are automorphisms. In fact, it is a very special loop in which this is the case.

Definition 2.14. A loop Q in which every inner mapping is an automorphism of Q is called an *automorphic loop*, or an *A-loop*.

Clearly groups are a variety of automorphic loops, but another important variety is called *commutative Moufang loops*. Moufang loops in general will be defined in more detail in chapter 5, but for now we define the commutative version as follows.

Definition 2.15. A loop Q is a *commutative Moufang loop*, or CML, if for every $x,y,z\in Q$,

$$xx\cdot yz=xy\cdot xz.$$

Chapter 3: Commutators in the variety of loops

3.1 Motivation

Since loop theory has both group theoretic and universal algebraic influences, it is no surprise that there have emerged differing definitions of what nilpotency and solvability should be for loops. It turns out that defining nilpotency in loops by mimicking the upper central series definition from group theory is equivalent to the iterated central extensions definition from universal algebra, which we will not expound on here. However, solvability is not so lucky.

Perhaps the most famous attempt at defining solvability in loops using group-theoretic intuition comes from Bruck [6], who defined the derived subloop of a loop using element-wise commutators and associators. While this definition was quite useful to Bruck in discovering important results for nilpotency and solvability in Moufang loops, it falls short when trying to generalize to the commutator of two normal subloops and consequently, to solvability in general loops. See Section §3.2 and [40] for more details.

On the other hand, the universal algebraic approach to commutators has been studied for more than 40 years, thanks to the initial theory set down by Smith [37], who laid out the notion of commutators for congruence permutable varieties. This was later generalized to congruence modular varieties by Freese and McKenzie [15], among others (Hagemann, Hermann, Gumm, Snow), who defined the commutator of two congruences using a term condition defined in §3.2. Over a decade later, Janelidze and Pedicchio examined the Freese-McKenzie commutator within the context of category theory. In [18], they developed an equivalent definition of the commutator in congruence permutable varieties based on the variety's Malcev terms as follows: the commutator of two congruences α and β in an algebra **A** in a congruence permutable variety is the smallest congruence δ such that the composition of maps

$$\varphi : \{(x, y, z) \in A^3 : x \, \alpha \, y \, \beta \, z\} \xrightarrow{p} A \to A/\delta$$

is a homomorphism, where p is a Malcev term in the variety. While this definition is perhaps more conceptual than the term condition, the proof of the equivalence of the Janelidze-Pedicchio commutator and the Freese-McKenzie commutator in [18] is category theoretic instead of universal algebraic.

The Freese-McKenzie term-condition commutator has proven to be useful in several applications and has been extended to even wider classes of varieties. We direct the reader to [30] for more details and some nice examples, specifically in the varieties of rings and lattices. In addition to the examples detailed in [30], the term condition definition of the commutator was used extensively in the recent work by Stanovský and Vojtěchovský ([40, 41]) to develop a detailed commutator theory within varieties of loops. The difficulty of working with the Freese-McKenzie commutator is that within loops, the term condition is cumbersome to work with. To alleviate this, Stanovský and Vojtěchovský found explicit generators for commutators within varieties of loops, a result described in more detail in §3.2 and §3.6 below.

The generators given by Stanovský and Vojtěchovský rely on a slightly unfamiliar object called the total inner mapping group of a loop. Although the total inner mapping group is easy enough to define, the commutator in loops would be more intuitively satisfying if it relied only on the inner mapping group, a more familiar group which is generally smaller than the total inner mapping group. Whether or not this can be done was explicitly stated as an open problem in [41].

We find that the most satisfying approach to answering the open problem is to use the definition of commutator as given by the Janelidze-Pedicchio Malcev term definition. After establishing some preliminaries in §3.2, we present in §3.3 another proof of the equivalence of the Freese-McKenzie and Janelidze-Pedicchio commutators. One direction of the proof works in general congruence permutable varieties, the other direction is specific to the variety of loops.

We then use the Janelidze-Pedicchio commutator to find more satisfying generators in §3.4. We introduce a new loop term we call a *mediator*. Mediators are analogous to element-wise associators and commutators, that is, a mediator measures how far a loop is from being *both* commutative and associative. Mediators turn out to give generators for commutators. Moreover, mediators are directly related to inner mappings, allowing us also to bypass the total inner mapping group completely and write the commutator in terms of just inner mappings. This answers in the affirmative the open question posed in [41]. In particular, we will prove the following theorem, where m is a specific mediator and F is a specific inner mapping, both defined in §3.4, and $C(\alpha, \beta; \delta)$ relates to the Freese-McKenzie term condition, defined in detail in §3.2:

Theorem 3.5. Let Q be a loop and α, β, and δ congruences on Q. Then the following are equivalent:

(a) $C(\alpha, \beta; \delta)$.

(b) The composition of maps $\varphi : \{(x, y, z) \in Q^3 : x \,\alpha\, y \,\beta\, z\} \xrightarrow{p} Q \to Q/\delta$ is a loop homomorphism, where p is the loop Malcev term $p(a, b, c) = a(b\backslash c)$.

(c) δ contains the congruence generated by all pairs $(m(x_1, x_2, b_1, b_2), m(y_1, y_2, b_1, b_2))$ where $x_i \,\alpha\, y_i$ and $b_i \,\beta\, 1$.

(d) δ contains the congruence generated by all $(L_{x_1,x_2}(b), L_{y_1,y_2}(b))$ and all $(F_{x_1,x_2}(b), F_{y_1,y_2}(b))$ such that $x_i \,\alpha\, y_i$ and $b \,\beta\, 1$.

In loops, congruences are in bijective correspondence with normal subloops, so in §3.5 we rephrase this main theorem to show that the commutator of two normal subloops can also be generated by mediators and inner mappings. The answer to the open problem of [40] presents new questions about whether or not this representation of the commutator in loops can help in solving other open problems, such as the question of whether congruence solvability and classical solvability coincide in certain varieties of loops.

3.2 Preliminaries

We begin this section with a slightly more in depth look at the problem of the commutator and solvability in loops, and then we will present the definitions needed for the representation of the commutator.

Recall that a group G is defined to be *solvable* if there exists a subnormal series $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ such that each G_{i+1}/G_i is an abelian group. Equivalently in group theory, we may say that G is solvable if its derived series terminates, where the derived series is defined recursively as follows. The derived subgroup of G is $G' = [G, G] = \langle [g, h] : g, h \in G \rangle$ where $[g, h] = ghg^{-1}h^{-1}$. Then we have $G^{(0)} = G$, $G^{(1)} = G'$, and $G^{(i+1)} = [G^{(i)}, G^{(i)}]$.

The project of Bruck [6] was to mimic this definition in the variety of Moufang loops in particular. However, since in loops we are not guaranteed associativity or two-sided inverses, some care must be taken to define what exactly is meant by $[a, b]$ for a and b in a loop Q. Moreover, in groups, G' is the smallest normal subgroup of G such that G/G' is an abelian group. If we want the same result for a loop Q, we must also make sure Q/Q' is associative, so there is some notion of an element-wise associator as well. In the literature, there are many different versions of what is meant by an element-wise associator or commutator in loops. For some a, b in a loop Q, we would like the commutator of a and b, $[a, b]$, to be a measure of commutativity – so it should vanish when a and b commute. One way to write this is that $[a, b]$ is the unique element such that $ab = ba \cdot [a, b]$. Similarly, the associator (a, b, c) should vanish when $a, b,$ and c associate. We make this explicit as follows.

Definition 3.1. For a loop Q and $a, b, c \in Q$, the *element-wise commutator of* a *and* b is

$$[a, b] = ba \backslash ab \,,$$

and the *element-wise associator of* $a, b,$ *and* c is

$$(a, b, c) = (a \cdot bc) \backslash (ab \cdot c) \,.$$

Then the *derived subloop of* Q, Q', is the normal subloop generated by all element-wise commutators and associators.

Notice that Q' here is the smallest normal subloop of Q such that Q/Q' is an abelian group. Then a loop solvable in this Bruck's sense if this derived series terminates. We will call this definition of solvability *classical solvability*.

The difference now arises from the notion of the commutator of two normal subloops. Here the derived series of a loop Q is being defined by the commutator of certain subloops H with themselves: $[H, H]$, and this is calculated by taking all of the element-wise commutators and associators with inputs from H as generators: $[a, b]$ where $a, b \in H$. This is what is called the "the commutator of H *in* H." However, the universal algebraic notion of solvability takes the commutator of two normal subloops within the context of the entire loop, that is, $[H, H]_Q$, which is "the commutator of H in Q," and creates an abelian series from these. If this series terminates, this is what we will refer to as *congruence solvability*. In groups, and indeed in Moufang loops as well, taking the commutator inside H versus inside the entire loop Q is equivalent. However, this is not true in general loops, where congruence solvability is strictly stronger than classical solvability [15]; i.e., being abelian inside the full loop is stronger than simply being abelian.

Classical solvability is often more intuitive, since the derived subloop is defined by taking specific terms and building up a subloop. The project started in [40] was to make congruence solvability just as intuitive by showing that the commutator of two normal subloops inside the full loop can also be generated by certain terms. In this chapter we simply taken the next step in this project, focusing on the commutator as defined in universal algebra.

First we start with some necessary definitions.

Definition 3.2. For a universal algebra $\mathbf{A}$, a *congruence* on $\mathbf{A}$ is an equivalence relation which respects all of the operations on $\mathbf{A}$.

Definition 3.3. For a universal algebra $\mathbf{A}$ and a set S of pairs of elements of A, the *congruence generated by* S, written $Cg(S)$, is the smallest set of pairs θ such that $S \subseteq \theta$ and θ is a congruence on $\mathbf{A}$.

Definition 3.4. A variety $\mathcal{V}$ is *congruence permutable* if for every algebra $\mathbf{A} \in \mathcal{V}$ and every pair of congruences θ, δ on $\mathbf{A}$, $\theta \circ \delta = \delta \circ \theta$, where $\circ$ is composition of binary relations.

Definition 3.5. A variety $\mathcal{V}$ is *congruence modular* if for every algebra $\mathbf{A} \in \mathcal{V}$, the lattice of congruences of $\mathbf{A}$ is a modular lattice.

We give this brief, unexplained definition of a congruence-modular variety because the work of Freese and McKenzie in [15] is primarily concerned with congruence-modular varieties. However, we are more interested in the stronger condition of congruence permutability in this chapter, and it is a well-known result that if a variety is congruence permutable, then it is congruence modular. For a proof, see [8]. Thus, Freese and McKenzie's results apply to congruence-permutable varieties, and an understanding of these more restricted varieties will suffice for the work done here.

Definition 3.6. Given a variety $\mathcal{V}$ and $\mathbf{A} \in \mathcal{V}$, an n-ary *term operation* t on $\mathbf{A}$ is a word-builder which takes as its input n letters from A and composes them using the operations from $\mathbf{A}$.

Example 3.1. For some $\mathbf{G}$ in the variety of groups, conjugation in G can be represented as a binary term operation: $t(x, a) = x \cdot a \cdot x^{-1}$.

Definition 3.7. Given a variety $\mathcal{V}$, $\mathcal{V}$ has a *Malcev term* if there is some term operation p in the variety satisfying $p(x, x, y) = p(y, x, x) = y$.

Example 3.2. Again in the variety of groups, the term operation $t(a, b, c) = a \cdot b^{-1} \cdot c$ is a Malcev term since $t(x, x, y) = y = t(y, x, x)$.

Congruence-permutable varieties are often referred to as *Malcev* varieties, since a variety is congruence-permutable if and only if it has a Malcev term. This is a well known result, for a proof, see [2]. It is not difficult to see that the variety of loops is congruence permutable (take $p(x, y, z) = x(y\backslash z)$ as one example of a Malcev term), and as such is also congruence-modular. Since the Freese-McKenzie commutator seems to be the correct lens with which to view commutator theory in loops, so we present it here as the definition of the commutator. We start with the following precursory definitions:

Definition 3.8. For $\mathbf{A}$ a universal algebra and α, β, δ congruences on $\mathbf{A}$, we say that α *centralizes* β *over* δ, and write $C(\alpha, \beta; \delta)$, if for every $(n+1)$-ary term operation t on $\mathbf{A}$, if $a \,\alpha\, b$ and $u_i \,\beta\, v_i$ for each $i \in \{1, \dots, n\}$, then

$$t(a, u_1, u_2, \dots, u_n) \,\delta\, t(a, v_1, v_2, \dots, v_n) \quad \Rightarrow \quad t(b, u_1, u_2, \dots, u_n) \,\delta\, t(b, v_1, v_2, \dots, v_n).$$

Given a specific term operation t, this implication is referred to as the *term condition for* t, written $\mathrm{TC}(t, \alpha, \beta, \delta)$.

We note that given a specific term t, it is not necessary that a be in the first slot. By defining a new term t', we may freely rearrange the order of the arguments for t and get an equivalent definition.

With these definitions in hand we may define the commutator as follows:

Definition 3.9. For **A** a universal algebra and α, β congruences on **A**, the *commutator of* α *and* β, $[\alpha, \beta]$, is the smallest congruence γ such that $C(\alpha, \beta; \gamma)$.

To illustrate this definition and show that it is a natural choice even in the variety of groups, we present the following example.

Example 3.3. Suppose that Q is a group and α, β congruences on Q. We associate normal subgroups A and B with the congruences α and β in the usual way, where $x\alpha y$ if and only if $xy^{-1} \in A$ and similarly $x \,\beta\, y$ if and only if $xy^{-1} \in B$. Let $a, b, u_1, u_2, v_1, v_2 \in Q$ such that $a \,\alpha\, b$, $u_i \,\beta\, v_i$, and consider the group term operation $t(x, y, z) = yxz$. To say that $TC(t, \alpha, \beta, \delta)$ is satisfied means that $(u_1 a u_2 \,\delta\, v_1 a v_2 \Rightarrow u_1 b u_2 \,\delta\, v_1 b v_2)$.

If we assume for a while that δ is equality, then this means that $(u_1 a u_2 = v_1 a v_2 \Rightarrow u_1 b u_2 = v_1 b v_2)$ or equivalently, $(a \cdot u_2 v_2^{-1} \cdot a^{-1} = u_1^{-1} v_1 \Rightarrow b \cdot u_2 v_2^{-1} \cdot b^{-1} = u_1^{-1} v_1)$. Noticing that $w_1 := u_1^{-1} v_1 \in B$ and $w_2 := u_2 v_2^{-1} \in B$, we define a map $T_a(x) := a^{-1} x a$, and see that the above implies that any two α-congruent elements act on the subgroup B in the same way. That is, $T_a(w) = T_b(w) \in B$ for any $w \in B$. Now $ab^{-1} \in A$, so $a^{-1} b \in A$, or alternatively, $b \in aA$. Since A is normal, it follows that $b \in Aa$, so we can write $b = ca$ for some $c \in A$. This implies that for any $a \in Q$, $c \in A$, and $w \in B$, $a^{-1} w a = a^{-1} c^{-1} w c a$, or $w = c^{-1} w c$, so $cw = wc$. Thus, if $C(\alpha, \beta; \delta)$, then we must have $cw \,\delta\, wc$. This implies that $[A, B]$ must contain the elements $[a, b] = a^{-1} b^{-1} a b$ such that $a \in A$ and $b \in B$, as is usual in group theory.

While this example is illustrative, it is incomplete. To be certain that $C(\alpha, \beta; \delta)$, we must have that $TC(t, \alpha, \beta, \delta)$ is satisfied for *every* choice of term t, which is by no means a simple task in general varieties, including loops. Given the power of the object and yet the difficulty of working with it, [40] set out to find generators for such a commutator in the variety of loops. To follow this construction, one must deal with an object called the total inner mapping group, which is defined as follows.

Definition 3.10. Let Q be a loop and define a map on Q by $M_x(y) = y\backslash x$. Then the *total multiplication group of* Q is

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

and the *total inner mapping group of* Q is the stabilizer of 1 in $\mathrm{TMlt}(Q)$.

With this, we may give the following generators for the commutator of two congruences, as presented in [40].

Theorem 3.1. [Stanovský and Vojtěchovský] Let $\mathcal{V}$ be a variety of loops and $\mathcal{W}$ a set of words that generates total inner mapping groups in $\mathcal{V}$. Then

$$[\alpha, \beta] = Cg((W_{\bar{u}}(a), W_{\bar{v}}(a)) : W \in \mathcal{W}, 1\,\alpha\,a, \bar{u}\,\beta\,\bar{v})$$

for any congruences α, β of any $Q \in \mathcal{V}$.

In [40], Stanovský and Vojtěchovský prove that the total inner mapping group in any variety of loops is generated by

$$\mathrm{TInn}(Q) = \langle L_{x,y}\,, R_{x,y}\,, M_{x,y}\,, T_x\,, U_x\ : x, y \in Q\rangle,$$

Where $M_{x,y} = M_{y\backslash x}^{-1} M_x M_y$ and $U_x = R_x^{-1} M_x$. Thus, in Theorem 3.1, we may take these generators to be the set $\mathcal{W}$.

This theorem is given in this section merely as motivation for the discussion which follows, as it will be presented in more depth in Section 3.6. While the work done in [40] greatly improved how the Freese-McKenzie commutator was understood, our goal is to present this same commutator in an even simpler way by using the power of the Malcev term to find generators in the inner mapping group instead.

3.3 The equivalence of two commutators

To begin this task, we acknowledge first the work of G. Janelidze and M.C. Pedicchio, who recognized and proved in [18] that the commutator of two congruences may be equivalently defined as the smallest congruence such that the composition of maps $\varphi : \{(x, y, z) \in A^3 : x\,\alpha\,y\,\beta\,z\} \xrightarrow{p} A \to A/\delta$ is a homomorphism, where A is a universal algebra in a congruence-permutable variety and p is some Malcev term in the variety. To emphasize what this means, as it will be used several times throughout this chapter, we take a specific algebra $\mathbf{A}$, α, β, δ congruences on $\mathbf{A}$, $x\,\alpha\,y\,\beta\,z \in A$, and $u\,\alpha\,v\,\beta\,w \in A$. To say that φ is a homomorphism means that $p(xu, yv, zw)\,\delta\,p(x, y, z)p(u, v, w)$. Being able to reduce the commutator to a problem of homomorphisms helps to simplify its characterization in terms of generators. Here we present a new proof of this equivalence, where the forward direction is viewed from inside universal algebra, and the converse from inside loop theory.

Theorem 3.2. Let $\mathcal{V}$ be a congruence-permutable variety, $\mathbf{A}$ an algebra in $\mathcal{V}$, and α, β, and δ congruences on $\mathbf{A}$. Suppose that the composition of maps $\varphi : \{(x, y, z) \in A^3 : x\,\alpha\,y\,\beta\,z\} \xrightarrow{p} A \to A/\delta$ is a homomorphism of algebras, where p is a Malcev term in the variety. Then $C(\alpha, \beta; \delta)$.

Proof. Let t be an $(n + 1)$-ary term operation on $\mathbf{A}$. Suppose $a, b \in A$ such that $a\,\alpha\,b$ and $u_i, v_i \in A$ such that $u_i\,\beta\,v_i$ for all $i = 1, 2, \ldots, n$. We assume that δ is a congruence such that φ is a homomorphism in $\mathcal{V}$ and that $t(a, u_1, u_2, \ldots, u_n)\,\delta\,t(a, v_1, v_2, \ldots, v_n)$. To simplify notation, we will denote congruence modulo δ by $\equiv$, $(u_1, \ldots, u_n)$ by $\vec{u}$, and

$(v_1, \ldots, v_n)$ by $\vec{v}$. In order to prove $C(\alpha, \beta; \delta)$, we must show that $t(b, \vec{u}) \equiv t(b, \vec{v})$. To start, we have:

$$\begin{aligned} t(b, \vec{u}) &= p(t(b, \vec{u}), t(a, \vec{u}), t(a, \vec{u})) && p \text{ is a Malcev term} \\ &\equiv p(t(b, \vec{u}), t(a, \vec{u}), t(a, \vec{v})) && t(a, \vec{u}) \equiv t(a, \vec{v}) \end{aligned}$$

Now φ being a homomorphism means we can, in a sense, commute φ with t. That is, given $x_i \,\alpha\, y_i \,\beta\, z_i$ for all $i \in \{1, 2, \ldots, n+1\}$:

$$\begin{gathered} \varphi(t(x_1, x_2, \ldots, x_{n+1}), t(y_1, y_2, \ldots, y_{n+1}), t(z_1, z_2, \ldots z_{n+1})) \\ = t(\varphi(x_1, y_1, z_1), \varphi(x_2, y_2, z_2), \ldots, \varphi(x_{n+1}, y_{n+1}, z_{n+1})) \end{gathered}$$

Since $a \,\alpha\, b$, we have $t(b, \vec{u}) \,\alpha\, t(a, \vec{u})$, and since $u_i \,\beta\, v_i$ for all $i \in \{1, 2, \ldots, n\}$, we have that $t(a, \vec{u}) \,\beta\, t(a, \vec{v})$. Thus, $t(b, \vec{u}) \,\alpha\, t(a, \vec{u}) \,\beta\, t(a, \vec{v})$, so $(t(b, \vec{u}), t(a, \vec{u}), t(a, \vec{v}))$ is in the domain of φ and it follows that

$$\begin{gathered} \varphi(t(b, u_1, u_2, \ldots, u_n), t(a, u_1, u_2, \ldots, u_n), t(a, v_1, v_2, \ldots, v_n)) \\ = t(\varphi(b, a, a), \varphi(u_1, u_1, v_1), \varphi(u_2, u_2, v_2), \ldots, \varphi(u_n, u_n, v_n)). \end{gathered}$$

Since φ sends triples to their δ-equivalence classes via p, this then shows that

$$t(b, \vec{u}) \equiv p(t(b, \vec{u}), t(a, \vec{u}), t(a, \vec{v})) \equiv t(p(b, a, a), p(u_1, u_1, v_1), \ldots, p(u_n, u_n, v_n)).$$

Employing the Malcev term, we have

$$t(p(b, a, a), p(u_1, u_1, v_1), \ldots, p(u_n, u_n, v_n)) = t(b, v_1, v_2, \ldots, v_n) = t(b, \vec{v}).$$

So $t(b,\vec{u}) \equiv t(b,\vec{v})$, as desired. □

While the converse holds in any congruence-permutable variety, as shown in [18], we return to the context of loops to present the following proof.

Theorem 3.3. Let Q be a loop and α, β, and δ congruences on Q such that $C(\alpha,\beta;\delta)$. Then the composition of maps $\varphi : \{(x,y,z) \in Q^3 : x\,\alpha\,y\,\beta\,z\} \xrightarrow{p} Q \to Q/\delta$ is a loop homomorphism where p is the loop Malcev term $p(a,b,c) = a(b\backslash c)$.

Proof. We will again use $\equiv$ to denote congruence modulo δ. Let $x\,\alpha\,y\,\beta\,z$ and $u\,\alpha\,v\,\beta\,w$ and define a term operation $m(a,b,c,d) = (ab)\backslash(ac{\cdot}bd)$. We use the fact proved in [15] that $C(\alpha,\beta;\delta)$ if and only if $C(\beta,\alpha;\delta)$. Now we have $m(y,v,1,1) = 1 = m(x,u,1,1)$, so certainly $m(y,v,1,1) \equiv m(x,u,1,1)$. Since $1\,\alpha\,1$, $x\,\alpha\,y$, $u\,\alpha\,v$, and $(y\backslash z)\,\beta\,1$, we employ the term condition TC(m,β,α,δ) to conclude that $m(y,v,y\backslash z,1) \equiv m(x,u,y\backslash z,1)$. Moreover, since $x\,\alpha\,y$, $u\,\alpha\,v$, $(y\backslash z)\,\alpha(y\backslash z)$, and $(v\backslash w)\,\beta\,1$, we again employ the term condition TC(m,β,α,δ) to conclude that

$$m(y,v,y\backslash z,v\backslash w) \equiv m(x,u,y\backslash z,v\backslash w).$$

By evaluating these terms, this then shows that

$$(yv)\backslash(y(y\backslash z)\cdot v(v\backslash w)) \equiv (xu)\backslash(x(y\backslash z)\cdot u(v\backslash w)).$$

We simplify to obtain $(yv)\backslash(zw) \equiv (xu)\backslash(x(y\backslash z)\cdot u(v\backslash w))$. Multiplying both sides on the left by xu, we have $(xu)((yv)\backslash(zw)) \equiv x(y\backslash z)\cdot u(v\backslash w)$. This is equivalent to $p(xu,yv,zw) \equiv p(x,y,z)p(u,v,w)$, so φ is a homomorphism of loops. □

Combining the results of Theorems 3.2 and 3.3, we have shown the following:

Corollary 3.4. Let p be the loop Malcev term $p(a, b, c) = a(b\backslash c)$. For a loop Q and α and β congruences on Q, the commutator $[\alpha, \beta]$ is the smallest congruence γ such that the composition of maps $\varphi : \{(x, y, z) \in Q^3 : x\,\alpha\,y\,\beta\,z\} \xrightarrow{p} Q \to Q/\gamma$ is a loop homomorphism.

The reader may notice that one direction of this equivalence was proved in general for any congruence permutable variety while the other direction made explicit use of certain properties of loops. It would be interesting to have a complete universal-algebraic proof for both directions for any congruence-permutable variety.

In light of the above corollary, we will freely use either definition of the commutator throughout the remainder of this paper.

3.4 Commutators and mediators

While the Malcev term characterization of the Freese-McKenzie commutator is perhaps more conceptual than its original definition, it is still difficult to use in practice. The goal of this section to describe the same commutator in terms of explicit generating pairs. Note that an essential role was played by the loop term operation $m(a, b, c, d)$ in the proof of Theorem 3.3. In this section, we give this term a name and show how it simplifies finding generating pairs for the commutator.

In group theory, a (syntactic) commutator measures how far a group is from being abelian, while in nonassociative algebra, associators measure how far algebras are from being associative. Borrowing an idea from quasigroup theory, we note that a loop is an abelian group if and only if it satisfies the *medial* (or entropic) identity $ab \cdot cd = ac \cdot bd$. We will define a mediator to be a loop term which measures how far a loop is from being medial. There are many possible conventions we could use. For example, the term $\mu(a, b, c, d) = (ab\backslash(ac \cdot bd))/cd$, which vanishes precisely when the medial identity holds, is a close analogy to commutator and associator terms. Notice that if $\mu(x_1, x_2, a, b) \equiv \mu(y_1, y_2, a, b)$ where $\equiv$ is some congruence, multiplying on the right by ab gives the equivalent $(x_1x_2)\backslash(x_1a \cdot x_2b) \equiv (y_1y_2)\backslash(y_1a \cdot y_2b)$. Since we will dealing mainly with terms of this form, we will adopt the latter as our definition.

Definition 3.11. Let Q be a loop and $a, b, c, d \in Q$. The *mediator* of a, b, c, d is the 4-ary term $m(a, b, c, d) = ab\backslash(ac \cdot bd)$.

This convention for mediators turns out to be a natural choice, because they are closely related to inner mappings, as the following discussion will show.

For $x, y \in Q$, we define a map $F_{x,y} : Q \to Q$ as $F_{x,y} = L_{xy}^{-1}R_yL_x$ and recall $L_{x,y} = L_{xy}^{-1}L_xL_y$ where L and R are the usual translation maps. Notice that $F_{x,y}(1) = 1$, so $F_{x,y}$ is indeed an inner mapping. With these definitions we come to the main result of this chapter, which relates these inner mappings to mediators and applies both concepts to our new (equivalent) definition of the commutator.

Theorem 3.5. Let Q be a loop and α, β, and δ congruences on Q. Then the following are equivalent:

(a) $C(\alpha, \beta; \delta)$.

(b) The composition of maps $\varphi : \{(x, y, z) \in Q^3 : x\,\alpha\,y\,\beta\,z\} \xrightarrow{p} Q \to Q/\delta$ is a loop homomorphism, where p is the loop Malcev term $p(a, b, c) = a(b\backslash c)$.

(c) δ contains the congruence generated by all pairs $(m(x_1, x_2, b_1, b_2), m(y_1, y_2, b_1, b_2))$ where $x_i\,\alpha\,y_i$ and $b_i\,\beta\,1$.

(d) δ contains the congruence generated by all pairs $(L_{x_1,x_2}(b), L_{y_1,y_2}(b))$ and $(F_{x_1,x_2}(b), F_{y_1,y_2}(b))$ such that $x_i\,\alpha\,y_i$ and $b\,\beta\,1$.

Proof. The equivalence of (a) and (b) is given by Theorems 3.2 and 3.3 in §3.3.

(b) $\implies$ (c): Suppose the homomorphism condition holds for δ and let x_1, x_2, y_1, y_2, b_1, and b_2 be in Q such that $x_i \,\alpha\, y_i$ and $b_i \,\beta\, 1$. Since $y_i \,\beta\, y_i b_i$, (b) implies that

$$p((x_1, y_1, y_1b_1)(x_2, y_2, y_2b_2)) \,\delta\, p(x_1, y_1, y_1b_1)p(x_2, y_2, y_2b_2)\,,$$

or equivalently,

$$x_1x_2 \cdot ((y_1y_2)\backslash(y_1b_1 \cdot y_2b_2)) \,\delta\, x_1(y_1\backslash y_1b_1) \cdot x_2(y_2\backslash y_2b_2) = x_1b_1 \cdot x_2b_2\,.$$

Dividing on the left by x_1x_2, and recalling the definition of m, we have

$$m(y_1, y_2, b_1, b_2) \,\delta\, m(x_1, x_2, b_1, b_2)\,.$$

Thus δ contains all pairs $(m(x_1, x_2, b_1, b_2), m(y_1, y_2, b_1, b_2))$ where $x_i \,\alpha\, y_i$ and $b_i \,\beta\, 1$, and, consequently, the congruence generated by such pairs.

(c) $\implies$ (d): For any $x, y, b \in Q$:

$$m(x, y, 1, b) = xy\backslash(x \cdot yb) = L_{xy}^{-1}L_xL_y(b) = L_{x,y}(b)$$

and

$$m(x, y, b, 1) = xy\backslash(xb \cdot y) = L_{xy}^{-1}R_yL_x(b) = F_{x,y}(b)\,.$$

Thus if (c) holds then certainly (d) holds as well.

(d) $\implies$ (b): To prove (b), we will prove

$$\varphi((u_1, v_1, w_1)(u_2, v_2, w_2)) = \varphi(u_1, v_1, w_1)\varphi(u_2, v_2, w_2)\,,$$

or equivalently

$$p(u_1u_2, v_1v_2, w_1w_2)\,\delta\,p(u_1, v_1, w_1)p(u_2, v_2, w_2)$$

for all $u_i\,\alpha\,v_i\,\beta\,w_i$, $i = 1, 2$. We first use (d) to prove two special cases:

1. If $x\,\alpha\,y\,\beta\,w$ and $z\,\alpha\,u$, then $p(x, y, w)\cdot z\,\delta\,p(xz, yu, wu)$.

2. If $x\,\alpha\,y$ and $z\,\alpha\,u\,\beta\,w$, then $x\cdot p(z, u, w)\,\delta\,p(xz, yu, yw)$.

For (1), we have

$$\begin{aligned} p(x, y, w)\cdot z &= x(y\backslash w)\cdot z \\ &= xz\cdot(xz)\backslash(x(y\backslash w)\cdot z) \\ &= xz\cdot F_{x,z}(y\backslash w) \\ &\delta\,xz\cdot F_{y,u}(y\backslash w) && \text{using (d) since } y\backslash w\,\beta\,1 \\ &= xz\cdot(yu\backslash wu) \\ &= p(xz, yu, wu)\,. \end{aligned}$$

For (2), we have

$$\begin{aligned} x\cdot p(z, u, w) &= x\cdot z(u\backslash w) \\ &= xz\cdot(xz)\backslash(x\cdot z(u\backslash w)) \\ &= xz\cdot L_{x,z}(u\backslash w) \\ &\delta\,xz\cdot L_{y,u}(u\backslash w) && \text{using (d) since } u\backslash w\,\beta\,1 \\ &= xz\cdot(yu\backslash yw) \\ &= p(xz, yu, yw)\,. \end{aligned}$$

Now let $u_i \,\alpha\, v_i \,\beta\, w_i$, $i = 1, 2$. Since $u_2 \,\alpha\, v_2$, we have $u_1u_2 \,\alpha\, u_1v_2$, and hence $u_1u_2/v_2 \,\alpha\, u_1$. Thus by (2),

$$\begin{aligned} u_1 \cdot p(u_2, v_2, w_2) \;&\delta\; p(u_1u_2, u_1u_2/v_2 \cdot v_2, u_1u_2/v_2 \cdot w_2) \\ &= p(u_1u_2, u_1u_2, u_1u_2/v_2 \cdot w_2) = u_1u_2/v_2 \cdot w_2 \,. \end{aligned} \tag{*}$$

Next, $u_2 \,\alpha\, v_2$ implies $u_2\backslash w_2 \,\alpha\, v_2\backslash w_2$, and thus

$$w_2 \,\alpha\, u_2 \cdot v_2\backslash w_2 = p(u_2, v_2, w_2) \,. \tag{**}$$

Next, $u_1 \,\alpha\, v_1$ and $u_2 \,\alpha\, v_2$ imply $u_1u_2 \,\alpha\, v_1v_2$, hence

$$u_1u_2/v_2 \;\alpha\; v_1 \,. \tag{***}$$

Similarly, $v_1 \,\beta\, w_1$ implies $v_1w_2 \,\beta\, w_1w_2$, so

$$w_2 \,\beta\, v_1\backslash w_1w_2 \,. \tag{†}$$

Moreover, $v_1 \,\beta\, w_1$ and $v_2 \,\beta\, w_2$ imply

$$v_2 \,\beta\, v_1\backslash w_1w_2 \,. \tag{‡}$$

Now we compute

$$\begin{aligned} p(u_1, v_1, w_1)p(u_2, v_2, w_2) \,&\delta\, p(u_1p(u_2, v_2, w_2), v_1w_2, w_1w_2) && \text{by (1) and (**)} \\ &\delta\, p(u_1u_2/v_2 \cdot w_2, v_1w_2, w_1w_2) && \text{by (*)} \\ &= p(u_1u_2/v_2 \cdot w_2, v_1w_2, v_1 \cdot v_1\backslash w_1w_2) \\ &\delta\, u_1u_2/v_2 \cdot p(w_2, w_2, v_1\backslash w_1w_2) && \text{by (2), (***) and (†)} \end{aligned}$$

$$
\begin{aligned}
&= u_1u_2/v_2 \cdot v_1\backslash w_1w_2 \\
&= u_1u_2/v_2 \cdot p(v_2, v_2, v_1\backslash w_1w_2) \\
&\delta\, p(u_1u_2/v_2 \cdot v_2, v_1v_2, v_1 \cdot v_1\backslash w_1w_2) \qquad \text{by (2), (***) and (‡)} \\
&= p(u_1u_2, v_1v_2, w_1w_2)\,.
\end{aligned}
$$

This completes the proof. □

Since the commutator is defined as the smallest congruence satisfying (a) or, equivalently (b), we have the following corollary.

Corollary 3.6. Let Q be a loop and α and β congruences on Q. Then

$$
\begin{aligned}
[\alpha, \beta] &= Cg((m(x_1, x_2, b_1, b_2), m(y_1, y_2, b_1, b_2)) : x_i\,\alpha\, y_i \text{ and } b_i\,\beta\, 1) \\
&= Cg((L_{x_1,x_2}(b), L_{y_1,y_2}(b)), (F_{x_1,x_2}(b), F_{y_1,y_2}(b)) : x_i\,\alpha\, y_i \text{ and } b\,\beta\, 1).
\end{aligned}
$$

Having now found a simpler characterization of the commutator of two congruences than its definition in terms of the term condition (or its Malcev term homomorphism characterization), we will translate this into a characterization of the commutator of two normal subloops in the next section.

3.5 The commutator of normal subloops

It is well known that the normal subloops of a loop Q are in bijective correspondence with the congruences of Q. This correspondence sends a congruence α to the block of α containing 1, which is a normal subloop of Q. Conversely, we may send any subloop A to the set of pairs (x, y) such that $y\backslash x \in A$, which forms a congruence on Q. Thus, having defined the commutator of two congruences, it is natural to define the commutator of two normal subloops of a loop.

Let A and B be normal subloops of a loop Q. Define a subset of Q^3 as follows:

$$S = \{(xa, x, xb) \mid a \in A, b \in B, x \in Q\}.$$

While this subset mimics the initial subloop in Theorem 3.5, it is not obvious that S forms a subloop of Q^3. However, we notice for $x, y \in Q$, $a_i \in A$, and $b_i \in B$:

$$(xa_1, x, xb_1)(ya_2, y, yb_2) = (xa_1 \cdot ya_2, xy, xb_1 \cdot yb_2)$$
$$= (xy \cdot [(xy)\backslash(xa_1 \cdot ya_2)], xy, xy \cdot [(xy)\backslash(xb_1 \cdot yb_2)]).$$

Since A and B are both normal subloops of Q, we see $(xy)\backslash(xa_1 \cdot ya_2) = (xy)\backslash(xy \cdot a') = a'$ for some $a' \in A$, and similarly $(xy)\backslash(xb_1 \cdot yb_2) = b'$ for some $b' \in B$. Thus, the expression above reduces to the triple $(xy \cdot a', xy, xy \cdot b') \in S$. Moreover, since A and B are normal subloops of Q, it follows that $xA\backslash yA = (x\backslash y)A$ and $xB\backslash yB = (x\backslash y)B$ for any $x, y \in Q$. Thus,

$$(xa_1, x, xb_1)\backslash(ya_2, y, yb_2) = (xa_1\backslash ya_2, x\backslash y, xb_1\backslash yb_2) = ((x\backslash y)a', x\backslash y, (x\backslash y)b')$$

for some $a' \in A$ and $b' \in B$. Thus, $(xa_1, x, xb_1)\backslash(ya_2, y, yb_2) \in S$. A dual argument shows that $(xa_1, x, xb_1)/(ya_2, y, yb_2) \in S$, so S is a subloop of Q^3.

Now we may define $[A, B]$ to be the smallest normal subloop C such that the composition of maps $S \xrightarrow{p} Q \to Q/C$ is a homomorphism of loops, where p is the usual Malcev term $p(x, y, z) = x(y\backslash z)$. To find a set of generators for this commutator, first note this composition is a homomorphism is equivalent to saying

$$p((xa_1, x, xb_1)(ya_2, y, yb_2)) \equiv p(xa_1, x, xb_1)p(ya_2, y, yb_2)$$

where congruence is modulo C. Equivalently,

$$\begin{aligned} p(xa_1 \cdot ya_2, xy, xb_1 \cdot yb_2) &= (xa_1 \cdot ya_2)((xy)\backslash(xb_1 \cdot yb_2)) \\ &\equiv (xa_1)(x\backslash(xb_1)) \cdot (ya_2)(y\backslash(yb_2)) \\ &= (xa_1 \cdot b_1)(ya_2 \cdot b_2)\,. \end{aligned}$$

Dividing on the left by $xa_1 \cdot ya_2$, this is then equivalent to

$$(xy)\backslash(xb_1 \cdot yb_2) \equiv (xa_1 \cdot ya_2)\backslash[(xa_1 \cdot b_1)(ya_2 \cdot b_2)]\,.$$

Recalling our loop term m, this shows

$$m(x, y, b_1, b_2) \equiv m(xa_1, ya_2, b_1, b_2)\,.$$

Thus, we get that the commutator of two normal subloops A and B of a loop Q is generated by all of the elements of the form $m(x, y, b_1, b_2)\backslash m(xa_1, ya_2, b_1, b_2)$. That is,

$$[A, B] = Ng(m(x, y, b_1, b_2)\backslash m(xa_1, ya_2, b_1, b_2) : x, y \in Q, a_i \in A, b_i \in B)\,.$$

Taking into account this discussion, we can state the subloop version of Theorem 3.5 as the following corollary.

Corollary 3.7. Let Q be a loop and A, B normal subloops of Q. Then the following are equivalent:

(a) The composition of maps $\varphi : \{(xa, x, xb) \mid a \in A, b \in B, x \in Q\} \xrightarrow{p} Q \to Q/C$ is a homomorphism of loops, where p is the usual Malcev term $p(x, y, z) = x(y\backslash z)$.

(b) C contains the normal subloop generated by all $m(x,y,b_1,b_2)\backslash m(xa_1,ya_2,b_1,b_2)$ where $x,y \in Q$ and $a_i \in A$ and $b_i \in B$.

(c) C contains the normal subloop generated by all $L_{x,y}(b)\backslash L_{xa_1,ya_2}(b)$ and all $F_{x,y}(b)\backslash F_{xa_1,ya_2}(b)$ such that $x,y \in Q$ and $a_i \in A$ and $b \in B$.

Again, in a style similar to Corollary 3.6, we see that the congruence of two normal subloops of a loop can be characterized as follows.

Corollary 3.8. Let Q be a loop and A, B normal subloops of Q. Then

$$\begin{aligned}[A,B] &= Ng(m(x,y,b_1,b_2)\backslash m(xa_1,ya_2,b_1,b_2) : x,y \in Q, a_i \in A, \text{ and } b_i \in B) \\ &= Ng(L_{x,y}(b)\backslash L_{xa_1,ya_2}(b), F_{x,y}(b)\backslash F_{xa_1,ya_2}(b) : x,y \in Q, a_i \in A \text{ and } b \in B)\end{aligned}$$

3.6 A note on total inner mappings

As stated previously, the Freese-McKenzie commutator has been widely used in loop theory to expound on many topics including nilpotency and solvability, the latter having different interpretations inside loops. One of the questions we wanted to try to answer is when these interpretations of solvability coincide inside loops and when they do not. Having a workable, straightforward approach to the commutator is essential to this project as well as many others in loop theory, a problem that was realized by Stanovský and Vojtěchovský. Thus, much work is done in [40, 41] to find generators for the Freese-McKenzie commutator, just as we have done above. However, without the use of mediators as this paper has detailed, they needed in [40, 41] to go through the total inner mapping group to find their generators. More specifically, they choose a set of mappings which together generate the total inner mapping group of a loop and use these mappings with inputs given specifically by the two congruences α and β in order to generate a congruence, which turns out to be the commutator of α and β. We present here a brief summary of their definitions and results in order to then answer the open question presented in [41] as to whether the total inner mapping group was necessary. In other words, is looking at just the inner mapping group enough? With the results from Theorem 3.5, we can answer this question in the affirmative, giving a simpler characterization of the commutator which may or may not prove to be easier to apply to other, larger open problems.

We again emphasize that what follows is only a summary of results from [40, 41], and direct the reader to these resources for proofs, calculations, and more details.

Recall that the total multiplication group of a loop Q is the permutation group on Q generated by the maps L_x, R_x, and M_x, where $L_x(a) = x \cdot a$, $R_x(a) = a \cdot x$, and $M_x(a) = a\backslash x$ for $x, a \in Q$, and the total inner mapping group is the stabilizer of 1 in the total multiplication group. Then a *tot-inner word* is defined to be a composition W of the maps L_x, R_y and M_z such that $x, y, z \in Q$ and $W(1) = 1$. With these definitions, we can then present the following characterizations of the commutator both as the commutator of two congruences (presented first in Section 3.2) and then as the commutator of two subloops.

Theorem 3.1. (Stanovský and Vojtěchovský) Let $\mathcal{V}$ be a variety of loops and $\mathcal{W}$ a set of words that generates total inner mapping groups in $\mathcal{V}$. Then

$$[\alpha, \beta] = Cg((W_{\bar{u}}(a), W_{\bar{v}}(a)) : W \in \mathcal{W}, 1\,\alpha\,a, \bar{u}\,\beta\,\bar{v})$$

for any congruences α, β of any $Q \in \mathcal{V}$.

Theorem 3.9. (Stanovský and Vojtěchovský) Let $\mathcal{W}$ be a set of tot-inner words such that for every loop Q we have $\mathrm{TInn}(Q) = \langle W_{\bar{u}} : W \in \mathcal{W}, u_i \in Q\rangle$. Let Q be a loop and A, B two normal subloops of Q. The commutator $[A, B]_Q$ is the smallest normal subloop of Q

containing the set

$$\{W_{\bar{u}}(a)/W_{\bar{v}}(a) : W \in \mathcal{W}, a \in A, u_i, v_i \in Q, u_i/v_i \in B\}.$$

As implied earlier, the power of Theorems 3.1 and 3.9 lies in converting the abstract concept of the Freese-McKenzie commutator in loops into a problem of finding generators for the total inner mapping group. In [40], the authors find several generating sets, and are able to eliminate certain mappings in more specific varieties of loops such as inverse property loops and commutative loops. For example, as previously noted, it can be shown that the total inner mapping group in any loop is generated as follows:

$$\text{TInn}(Q) = \langle L_{x,y}, R_{x,y}, M_{x,y}, T_x, U_x : x, y \in Q\rangle$$

where $M_{x,y} = M_{y\backslash x}^{-1} M_x M_y$ and $U_x = R_x^{-1} M_x$. Thus, finding the commutator of two congruences α and β reduces to finding the congruence generated by all pairs $(W_{\bar{u}}(a), W_{\bar{v}}(a))$ where $W \in \{L_{x,y}, R_{x,y}, M_{x,y}, T_x, U_x\}$, $1 \,\alpha\, a$, and $\bar{u} \,\beta\, \bar{v}$.

This characterization of the Freese-McKenzie commutator was used in [41] to prove many things about abelianness and centrality, but may have its drawbacks when considering the characterization of abelian normal subloops. Thus, the problem was presented in that same paper as Problem 4.3, stated here:

Problem 3.1. Does Theorem 3.1 remain true if “tot-inner” and “TInn(Q)” are replaced by “inner” and “Inn(Q)” in the condition imposed on the set $\mathcal{W}$ that is used for generating the commutator?

To answer this problem, we first show that the mappings $L_{x,y}$ and $F_{x,y}$ are all that are needed to generate the inner mapping group.

Lemma 3.10. Let Q be a loop. Then

$$\text{Inn}(Q) = \langle L_{x,y}, F_{x,y} : x, y \in Q \rangle.$$

Proof. It is well known that the inner mapping group is generated by $L_{x,y}$, $R_{x,y}$, and T_x for $x, y \in Q$. Thus, it suffices to show that each $R_{x,y}$ and T_x can be written as a composition of only $L_{a,b}$ and $F_{c,d}$ for some $a, b, c, d \in Q$. For any $x, y \in Q$ we have:

$$F_{x,y} = L_{xy}^{-1} R_y L_x = L_{xy}^{-1} R_{xy} R_{xy}^{-1} R_y R_x R_x^{-1} L_x = T_{xy}^{-1} R_{y,x} T_x$$

Letting $x = 1$, this shows that $F_{1,y} = T_y^{-1}$, so it follows that $T_y = F_{1,y}^{-1}$ for any $y \in Q$. Further, the two identities above give us that $R_{x,y} = T_{yx} F_{y,x} T_y^{-1} = F_{1,yx}^{-1} F_{y,x} F_{1,y}$ for any $x, y \in Q$. Since both T_x and $R_{x,y}$ can be represented in terms of $F_{x,y}$, it follows that

$$\text{Inn}(Q) = \langle L_{x,y}, F_{x,y} : x, y \in Q \rangle.$$

□

We now answer Problem 3.1 in the affirmative, stated formally in the following two corollaries.

Corollary 3.11. Let $\mathcal{V}$ be a variety of loops and $\mathcal{W}$ a set of words that generates inner mapping groups in $\mathcal{V}$. Then

$$[\alpha, \beta] = Cg((W_{\bar{u}}(a), W_{\bar{v}}(a)) : W \in \mathcal{W}, 1 \,\alpha\, a, \bar{u} \,\beta\, \bar{v})$$

for any congruences α, β of any $Q \in \mathcal{V}$.

Proof. Consider $\mathcal{W} = \{L_{x,y}, F_{x,y}\}$, and let α, β be congruences on $Q \in \mathcal{V}$. Lemma 3.10 shows that certainly $\mathcal{W}$ generates inner mapping groups and Corollary 3.6 gives us that

$[\alpha, \beta] = Cg((W_{x_1,x_2}(b), W_{y_1,y_2}(b)) : W \in \mathcal{W}, x_i \,\alpha\, y_i$ and $b \,\beta\, 1)$. Now notice that, since the commutator is symmetric, we have $[\alpha, \beta] = [\beta, \alpha]$, so $[\alpha, \beta] = Cg((W_{x_1,x_2}(b), W_{y_1,y_2}(b)) : W \in \mathcal{W}, x_i \,\beta\, y_i$ and $b \,\alpha\, 1)$. Thus, the statement holds for a certain generating set.

Now Lemmas 3.13 and 4.2 in [40] give that for $\delta = Cg((W_{\bar{u}}(a), W_{\bar{v}}(a)) : W \in \mathcal{W}, 1 \,\alpha\, a, \bar{u} \,\beta\, \bar{v})$ and V an inner word, $(V_{\bar{u}}(a), V_{\bar{v}}(a)) \in \delta$ for every $a \,\alpha\, 1, \bar{u} \,\beta\, \bar{v})$. Thus, it follows that if the statement holds for a certain generating set, it holds for all generating sets, which concludes the proof. □

In the subloop case, the following corollary is a similar restatement of Corollary 3.8, taking $\mathcal{W} = \{L_{x,y}, F_{x,y}\}$ as before. We note as well that while [41] defines the congruence of two subloops using the right division, the definition here using left divisions is dual.

Corollary 3.12. Let $\mathcal{W}$ be a set of inner words such that for every loop Q we have $\mathrm{Inn}(Q) = \langle W_{\bar{u}} : W \in \mathcal{W}, u_i \in Q \rangle$. Let Q be a loop and A, B two normal subloops of Q. The commutator $[A, B]_Q$ is the smallest normal subloop of Q containing the set

$$\{W_{\bar{u}}(a) \backslash W_{\bar{v}}(a) : W \in \mathcal{W}, a \in A, u_i, v_i \in Q, u_i \backslash v_i \in B\}.$$

3.7 Questions for further study

With this new characterization of the commutator, the question arises whether or not it simplifies the calculations necessary to prove other conjectures about abelianness and centrality, particularly those posed in [41]. Moreover, does this new characterization of the commutator help in answering problems about when classical and congruence solvability coincide?

Chapter 4: Quaternionic automorphic loops

4.1 Introduction

Recall that a loop is *automorphic* if all of its inner mappings are automorphisms of the loop. That is, for a loop Q, $\mathrm{Inn}(Q) \leq \mathrm{Aut}(Q)$. Bruck and Paige pioneered the study of automorphic loops in 1956. While proving important facts about automorphic loops in general, they were mostly concerned with diassociative automorphic loops, or loops in which every two-generated subloop is a group. The development of the general structure theory for automorphic loops came later, first with commutative automorphic loops in [19] and then for automorphic loops in general in [28]. We cite here only the essential results from automorphic loop theory, and direct the reader to [28, 19, 7] for proofs and a more thorough treatment of the topic.

It is perhaps important to note that commutative Moufang loops and groups are both varieties of automorphic loops. Thus, many properties of automorphic loops are reminiscent of these two varieties.

Definition 4.1. Let Q be a loop. Q is *power-associative* if every one-generated subloop of Q is a group.

Lemma 4.1. (Bruck, Paige [7]) Every automorphic loop is power-associative.

Since powers associate in an automorphic loop, we may use exponent notation unambiguously. That is, $x^n = \underbrace{x \cdot x \cdot \cdots \cdot x}_{n}$ and the usual multiplication rule for exponents holds: $x^n x^m = x^{n+m}$. Once we have exponents, we would like to be able to freely use the notation x^{-1}. In loops in general, we are not guaranteed that every element has a unique two-sided inverse, so this notation would be ambiguous. However, in automorphic loops, we may use this notation. In fact, we get even more.

Definition 4.2. A loop Q has the *antiautomorphic inverse property* (AAIP) if every element has a two-sided inverse and for every $x, y \in Q$,

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Lemma 4.2. (Johnson, Kinyon, Nagy, Vojtěchovský [22]) Every automorphic loop has the AAIP.

Lemma 4.3. (Kinyon, Kunen, Phillips, Vojtěchovský [28]) Let Q be an automorphic loop and $x, y \in Q$. Then

$$\begin{aligned} R_{x,y} &= L_{x^{-1},y^{-1}} \\ T_x^{-1} &= T_{x^{-1}}. \end{aligned}$$

In particular, this lemma implies that in any automorphic loop Q,

$$\mathrm{LInn}(Q) = \mathrm{RInn}(Q). \tag{4.1}$$

Another consequence of Lemma 4.2 is the following:

Lemma 4.4. (Kinyon, Kunen, Phillips, Vojtěchovský [28]) Let Q be an automorphic loop. Then

(i) $N_\lambda(Q) = N_\rho(Q) \subseteq N_\mu(Q)$, and

(ii) each nucleus is normal in Q.

Since the focus of this chapter is on the nonassociative generalization of the generalized quaternion groups, it may be helpful to begin with the group construction.

4.1.1 Generalized quaternion groups.

4.1.1 Generalized quaternion groups. With the dihedral group, D_8, of order 8, the only other noncommutative group of order 8 is the quaternion group, Q_8. It is classically constructed with two generators, i and j, such that $jij^{-1} = i^{-1}$ and $i^2 = j^2 = -1$. Notice this latter condition implies $i^4 = j^4 = 1$. We also recall the presentation of the dihedral group D_8 with two generators, r and s such that $r^4 = s^2 = 1$ and $srs^{-1} = r^{-1}$, and note that these two groups appear to have some similarities. In fact, they can both be constructed from a semi-direct product in a similar way. For D_8, take the semi-direct product $H := \mathbb{Z}_4 \rtimes \mathbb{Z}_2$, where $\mathbb{Z}_2$ acts on $\mathbb{Z}_4$ by identity and negation. That is,

$$(a, b)(c, d) = (a + (-1)^b c, b + d).$$

Then $D_8 \cong H$.

While the quaternion group cannot be written as a semi-direct product (there are no two proper, nontrivial subgroups with trivial intersection), it can be constructed as a quotient of a semi-direct product. More specifically, take the group $G := \mathbb{Z}_4 \rtimes \mathbb{Z}_4$ with multiplication given by

$$(a, b)(c, d) = (a + (-1)^b c, b + d).$$

Then the element $(2, 2)$ is in $Z(G)$ and has order 2, so $\langle (2, 2) \rangle \trianglelefteq G$. The result is then that $Q_8 \cong G/\langle (2, 2) \rangle$. This is a known group theory fact, for a proof see [9].

This construction can be extended to higher orders as follows. Take the semidirect product $G := \mathbb{Z}_{2^{n-1}} \rtimes \mathbb{Z}_4$ for $n \geq 3$ with multiplication given by

$$(a, b)(c, d) = (a + (-1)^b c, b + d).$$

Now the element $(2^{n-2}, 2)$ is in $Z(G)$ and has order 2, so it makes sense to construct the *generalized quaternion group* of order 2^n by $Q_{2^n} = G/\langle (2^{n-2}, 2) \rangle$.

We list here some known properties of these generalized quaternion groups as motivation and reference for their nonassociative analogs, and again direct the reader to [9] for proofs.

Theorem 4.5. Let Q_{2^n} be a generalized quaternion group of order 2^n and let $x = \overline{(1,0)}$ and $y = \overline{(0,1)}$ in Q_{2^n}. Then:

1. $Q_{2^n} = \langle x, y \rangle$.

2. Every element of Q_{2^n} can be written in the form x^a or $x^a y$ for some $a \in \mathbb{Z}$.

3. $x^{2^{n-2}} = y^2$ and is the unique element of order 2.

4. For every $g \in Q_{2^n}$ such that $g \notin \langle x \rangle$, $gxg^{-1} = x^{-1}$.

5. The center of Q_{2^n} is $\{1, x^{2^{n-2}}\}$ and $Q_{2^n}/Z(Q_{2^n}) \cong D_{2^{n-1}}$.

6. For $n \geq 3$, let $H := \langle a, b \rangle$ such that $a^{2^{n-1}} = b^4 = 1$, $bab^{-1} = a^{-1}$, and $a^{2^{n-2}} = b^2$. There is a unique homomorphism $\psi : Q_{2^n} \to H$ such that $x \mapsto a$, $y \mapsto b$, and ψ is onto. If $|H| = 2^n$ then ψ is an isomorphism.

7. The subgroup $\langle x \rangle$ has index 2 and every element outside of $\langle x \rangle$ has order 4.

8. For $n \geq 4$, the noncyclic proper normal subgroups of Q_{2^n} are $\langle x^2, y \rangle$ and $\langle x^2, xy \rangle$, both of which have index 2 and are isomorphic to $Q_{2^{n-1}}$.

9. Every subgroup of Q_{2^n} is cyclic or generalized quaternion.

4.1.2 Dihedral-like automorphic loops. Since not many specific examples of automorphic loops are known, there is a desire to find constructions which produce automorphic loops. One such effort was started by Kinyon, Kunon, Phillips, and Vojtěchovský, who did an extensive study of automorphic loops in [28] and constructed what they call *dihedral automorphic loops*. This work was generalized by Aboras in [1], who defined *dihedral-like* *automorphic loops*. Since dihedral automorphic loops are a special case of their dihedral-like relatives, we present first the definition of a dihedral-like automorphic loop.

Definition 4.3. Let m be a positive even integer, G an abelian group, and φ an automorphism of G that satisfies $\varphi^2 = 1$ if $m > 2$. Then the *dihedral-like automorphic loop*, written Dih(m, G, φ) is defined on $G \times \mathbb{Z}_m$ by

$$(u,i)(v,j) = (\varphi^{ij}(u + (-1)^i v), i + j).$$

The special case when $m = 2$ is called a *dihedral automorphic loop*.

Notice if $m = 2$, $G = \mathbb{Z}_n$, and $\varphi = 1$, Dih$(2, \mathbb{Z}_n, 1)$ is the dihedral group of order $2n$, making this construction the "correct" generalization of the dihedral groups to the automorphic loop setting.

4.2 Construction of quaternionic automorphic loops

Inspired by the construction of the generalized quaternion groups and the dihedral-like automorphic loops, we construct the quaternionic automorphic loops of order 2^n for $n \geq 3$ as follows. Consider $G := \mathbb{Z}_{2^{n-1}} \times \mathbb{Z}_4$ for $n \geq 3$ and let $\varphi \in \mathrm{Aut}(\mathbb{Z}_{2^{n-1}})$ such that $\varphi^2 = 1$. Build a loop D on the underlying set of G with multiplication given by:

$$(a,b)(c,d) = (\varphi^{bd}(a + (-1)^b c), b + d).$$

By work done in [1], D is an automorphic loop of order 2^{n+1}, i.e., a dihedral-like automorphic loop.

Lemma 4.6. Given the loop D of order 2^{n+1} constructed as above, the element $(2^{n-2}, 2)$ has order 2 and is in the center of D.

Proof. To show that $(2^{n-2}, 2)$ has order 2, we calculate, recalling that the first coordinate is calculated in $\mathbb{Z}_{2^{n-1}}$ and the second coordinate is calculated in $\mathbb{Z}_4$:

$$(2^{n-2}, 2)(2^{n-2}, 2) = (\varphi^4(2^{n-2} + (-1)^2 \cdot 2^{n-2}), 0) = (0, 0)$$

To show that $(2^{n-2}, 2)$ is in the commutant, take $(a, b) \in D$ and calculate:

$$(2^{n-2}, 2)(a, b) = (\varphi^{2b}(2^{n-2} + (-1)^2 a), 2 + b) = (2^{n-2} + a, 2 + b)$$

and also:

$$(a, b)(2^{n-2}, 2) = (\varphi^{2b}(a + (-1)^b 2^{n-2}), b + 2) = (a \pm 2^{n-2}, b + 2).$$

Since $2^{n-2} = -2^{n-2}$ we have $(2^{n-2} + a, 2 + b) = (a + 2^{n-2}, b + 2)$. It follows that $(2^{n-2}, 2) \in C(D)$. Since D is a dihedral-like automorphic loop, we have from [1] that $N_\lambda(D) = \text{Fix}(\varphi) \times \langle 2 \rangle$, where $\text{Fix}(\varphi)$ is the set of fixed points of φ. Now φ is acting on $\mathbb{Z}_{2^{n-1}}$ and 2^{n-2} is the unique element of order 2 in $\mathbb{Z}_{2^{n-1}}$, so it is fixed by all automorphisms of $\mathbb{Z}_{2^{n-1}}$. Specifically, $2^{n-2} \in \text{Fix}(\varphi)$. Certainly $2 \in \langle 2 \rangle$, so it follows that $(2^{n-2}, 2) \in N_\lambda(D) = N(D)$ and thus, $(2^{n-2}, 2) \in Z(D)$. □

Now, since $(2^{n-2}, 2)$ has order 2 and is in the center, $\langle (2^{n-2}, 2) \rangle$ is a normal subloop of D of order 2, so it makes sense to construct the factor loop $Q = D/\langle (2^{n-2}, 2) \rangle$. Since automorphic loops form a variety, Q is an automorphic loop of order $2^{n+1}/2 = 2^n$. We call loops constructed in this way *quaternionic automorphic loops*.

There are three automorphisms of $\mathbb{Z}_{2^{n-1}}$ of order 2 for $n > 3$ [12, Corollary 9.20]. Considered as invertible elements of the ring $(\mathbb{Z}_{2^{n-1}}, +\cdot)$, these are $\iota := -1$, $\alpha := 2^{n-2} - 1$, and $\beta := 2^{n-2} + 1$. We will thus interpret $\varphi(a)$ as simply $\varphi \cdot a \mod 2^{n-1}$ for $\varphi \in \{\alpha, \beta, \iota\}$.

4.2.1 Notation. Each of the three automorphisms of $\mathbb{Z}_{2^{n-1}}$ produce a distinct quaternionic automorphic loop of order 2^n for $n > 3$, as we shall prove in §4.5. As such, we use the following notation convention to distinguish which automorphism was used in the construction.

$$Q^{\iota}_{2^n} \text{ is the loop of order } 2^n \text{ constructed with } \iota = -1.$$

$$Q^{\alpha}_{2^n} \text{ is the loop of order } 2^n \text{ constructed with } \alpha = 2^{n-2} - 1.$$

$$Q^{\beta}_{2^n} \text{ is the loop of order } 2^n \text{ constructed with } \beta = 2^{n-2} + 1.$$

In what follows, it is always assumed that the automorphism φ used in the construction is in $\mathrm{Aut}(\mathbb{Z}_{2^{n-1}})$ where $n \geq 3$ and has order 2. When not specified to be $\alpha, \beta,$ or ι, $Q^{\varphi}_{2^n}$ is the quaternionic automorphic loop of order 2^n constructed with any $\varphi \in \{\alpha, \beta, \iota\}$.

4.3 Precursory calculations

As we will show later, there are two important elements of any quaternionic automorphic loop and a third which will prove useful. We give them names here as follows:

$$\mathbf{x} := \overline{(1,0)} \qquad \text{and} \qquad \mathbf{y} := \overline{(0,1)} \qquad \text{and} \qquad \mathbf{z} := \overline{(1,1)}\,.$$

For what follows in this chapter, it will be useful to state a few facts about parity in general and also parity in the context of a quaternionic automorphic loop. These may be used in later proofs without reference.

Lemma 4.7. Let $Q = Q^{\varphi}_{2_n}$ be a quaternionic automorphic loop of order 2^n.

1. For any $a \in \mathbb{Z}$, $a^2 \equiv a \mod 2$ and $-a \equiv a \mod 2$.

2. For any $a \in \mathbb{Z}$, $-a \equiv a \mod 2^{n-1}$ if and only if ($a \equiv 0 \mod 2^{n-1}$ or $a \equiv 2^{n-2} \mod 2^{n-1}$).

3. For any $\overline{(a,b)} \in Q$, φ preserves the parity of a. Moreover, α acts as inversion on even first coordinates and β acts as the identity on even first coordinates.

4. Let $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(k, b+d)} \in Q$ where $k = \varphi^{bd}(a + (-1)^b c)$. If a, c are both even or both odd, then k is even. If exactly one of a or c is even (and the other odd), then k is odd.

Proof. Both (1) and (2) are modular arithmetic facts. For (3), we recall that calculations in the first coordinate are taken modulo 2^{n-1}, so we calculate:

$$\alpha(2m) = (2^{n-2} - 1)(2m) = 2^{n-1}m - 2m = -2m\,,$$

$$\iota(2m) = -2m\,,$$

$$\beta(2m) = (2^{n-2} + 1)(2m) = 2^{n-1}m + 2m = 2m\,.$$

Moreover, for an odd number $2m+1$ in the first coordinate, the result is also odd:

$$\alpha(2m+1) = (2^{n-2} - 1)(2m+1) = 2^{n-1}m - 2m + 2^{n-2} - 1 = 2(2^{n-3} - m) - 1\,,$$

$$\iota(2m+1) = -2m - 1\,,$$

$$\beta(2m+1) = (2^{n-2} + 1)(2m+1) = 2^{n-1}m + 2m + 2^{n-2} + 1 = 2(2^{n-3} + m) + 1\,.$$

Lastly, for part (4), we have from part (3) that φ preserves parity. Thus, if both a and c share the same parity, then their sum (or difference) is even so $\varphi(a + (-1)^b c)$ is also even. Similarly, if a and c have different parities, then their sum (or difference) is odd, giving that k is also odd, as desired. □

Whenever a new multiplication is defined, it is helpful to see how each of the other loop operations as well as the inner mappings are affected. We present here some of these calculations which will be used extensively and not necessarily with reference in later proofs. Note that the following calculations hold in any dihedral-like automorphic loop constructed as in §4.2. Since automorphic loops form a variety, then these equations also hold in the corresponding quaternionic automorphic loop.

Lemma 4.8. For any automorphism φ of order 2 used in the construction of a quaternionic automorphic loop of order 2^n, the following identities hold:

$$(c,d)/(u,v) = (\varphi^{dv+v}(c) + (-1)^{d-v+1}u, d-v) \tag{4.2}$$

$$(c,d)\backslash(u,v) = ((-1)^d\varphi^{dv+d}(u) + (-1)^{d+1}c, v-d) \tag{4.3}$$

$$T_{(u,v)}(a,b) = ((1+(-1)^{b+1})u + (-1)^v a, b) \tag{4.4}$$

$$T_{\mathbf{x}}(a,b) = ((1+(-1)^{b+1}) + a, b) \tag{4.5}$$

$$T_{\mathbf{x}}^u(a,b) = ((1+(-1)^{b+1})u + a, b) \tag{4.6}$$

$$T_{\mathbf{y}}(a,b) = (-a, b) \tag{4.7}$$

$$T_{\mathbf{y}}^v(a,b) = ((-1)^v a, b) \tag{4.8}$$

$$T_{(u,v)}^{-1}(a,b) = (((-1)^{v+b} + (-1)^{v+1})u + (-1)^v a, b) \tag{4.9}$$

$$T_{\mathbf{x}}^{-1}(a,b) = (((-1)^{b} + (-1)) + a, b) \tag{4.10}$$

$$R_{(x_1,y_1),(x_2,y_2)}(a,b) = ((-1)^{b+y_2}\varphi^{y_2y_1}(\varphi^{by_2}(x_1) - x_1) + \varphi^{y_2y_1}(a), b). \tag{4.11}$$

$$R_{\mathbf{x},(x_2,y_2)}(a,b) = ((-1)^{b+y_2}(\varphi^{by_2}(1) - 1) + a, b) \tag{4.12}$$

$$R^{x_1}_{\mathbf{x},(x_2,y_2)}(a,b) = ((-1)^{b+y_2}(\varphi^{by_2}(1) - 1)x_1 + a, b) \tag{4.13}$$

$$R_{\mathbf{x},\mathbf{z}}(a,b) = ((-1)^{b+1}(\varphi^{b}(1) - 1) + a, b) \tag{4.14}$$

$$R^{x_1}_{\mathbf{x},\mathbf{z}}(a,b) = ((-1)^{b+1}(\varphi^{b}(x_1) - x_1) + a, b) \tag{4.15}$$

$$R_{\mathbf{y},(x_2,y_2)}(a,b) = (\varphi^{y_2}(a), b) \tag{4.16}$$

$$R^{y_1}_{\mathbf{y},(x_2,y_2)}(a,b) = (\varphi^{y_1y_2}(a), b) \tag{4.17}$$

$$R_{\mathbf{y},\mathbf{z}}(a,b) = (\varphi(a), b) \tag{4.18}$$

$$R^{y_1}_{\mathbf{y},\mathbf{z}}(a,b) = (\varphi^{y_1}a, b) \tag{4.19}$$

Proof. For (4.2), let $(c,d)/(u,v) = (a,b)$, then $(a,b)(u,v) = (c,d)$. Calculating the left side of this equation gives us $(\varphi^{bv}(a+(-1)^b u), b+v)$. Setting $b+v = d$, we see first that $b = d-v$. Thus, $\varphi^{(d-v)v}(a+(-1)^{d-v}u) = c$. Since φ has order 2, $\varphi^{(d-v)v} = \varphi^{dv+v}$, so we rewrite $\varphi^{dv+v}(a+(-1)^{d-v}u) = c$. Solving for a gives $a = \varphi^{dv+v}(c) + (-1)^{d-v+1}u$. Thus, $(c,d)/(u,v) = (\varphi^{dv+v}(c) + (-1)^{d-v+1}u, d-v)$, as desired.

For (4.3), let $(c,d)\backslash(u,v) = (a,b)$, then $(c,d)(a,b) = (u,v)$. So $u = \varphi^{db}(c+(-1)^d a)$ and $v = d+b$. Thus, $b = v-d$ so substituting and using the fact that φ has order 2, $u = \varphi^{dv+d}(c+(-1)^d a)$. Solving for a yields $a = (-1)^d\varphi^{dv+d}(u) + (-1)^{d+1}c$, as desired.

For (4.4) we have

$$T_{(u,v)}(a,b) = [(u,v)(a,b)]/(u,v) = (\varphi^{vb}(u+(-1)^v a), v+b)/(u,v).$$

Using (4.2), this is equal to

$$(\varphi^{(v+b)v+v}(\varphi^{vb}(u+(-1)^v a)) + (-1)^{v+b-v+1}u, v+b-v).$$

Since φ has order 2, this reduces to $(\varphi^{v^2+v}(u+(-1)^v a)+(-1)^{b+1}u, b)$. We notice $v^2+v = v(v+1)$ which is an odd times an even, making v^2+v an even number. Again, since φ has order 2, φ^{v^2+v} then reduces to the identity, so we have $(u+(-1)^v a+(-1)^{b+1}u, b)$ or equivalently $((1+(-1)^{b+1})u+(-1)^v a, b)$, as desired.

It is straightforward to see that (4.5) and (4.7) are just applications of (4.4). For (4.6), we proceed by induction on u. The case where $u = 1$ is just (4.5), so suppose the equality holds for all positive integers less than u. Then

$$\begin{aligned} T_{\mathbf{x}}^u(a,b) &= T_{\mathbf{x}}^{u-1}T_{\mathbf{x}}(a,b) \\ &= T_{\mathbf{x}}^{u-1}((1+(-1)^{b+1})+a, b) \end{aligned}$$

$$= ((1 + (-1)^{b+1})(u-1) + (1 + (-1)^{b+1}) + a, b)$$
$$= ((1 + (-1)^{b+1})u + a, b).$$

Similarly for (4.8), we proceed by induction on v. The case where $v = 1$ is given by (4.7), so suppose that the equality holds for all positive integers less than v. Then

$$T_{\mathbf{y}}^{v}(a, b) = T_{\mathbf{y}}^{v-1} T_{\mathbf{y}}(a, b) = T_{\mathbf{y}}^{v-1}(-a, b) = ((-1)^{v-1}(-a), b) = ((-1)^{v} a, b).$$

For (4.9), we have

$$T_{(u,v)}^{-1}(a, b) = L_{(u,v)}^{-1} R_{(u,v)}(a, b) = (u, v)\backslash[(a, b)(u, v)] = (u, v)\backslash(\varphi^{bv}(a + (-1)^{b} u), b + v).$$

Using (4.3), this is equal to

$$((-1)^{v} \varphi^{v(b+v)+v}(\varphi^{bv}(a + (-1)^{b} u)) + (-1)^{v+1} u, b + v - v).$$

Simplifying using the fact that φ has order 2, we get $((-1)^{v} a + (-1)^{v+b} u + (-1)^{v+1} u, b)$, as desired. Then (4.10) is simply an application of this equality.

For (4.11), we calculate:

$$R_{(x_1,y_1),(x_2,y_2)}(a, b)$$
$$= [(a, b)(x_2, y_2) \cdot (x_1, y_1)]/[(x_2, y_2)(x_1, y_1)]$$
$$= [(\varphi^{by_2}(a + (-1)^{b} x_2), b + y_2)(x_1, y_1)]/(\varphi^{y_2 y_1}(x_2 + (-1)^{y_2} x_1), y_2 + y_1)$$
$$= (\varphi^{by_1 + y_1 y_2}(\varphi^{by_2}(a + (-1)^{b} x_2) + (-1)^{b+y_2} x_1), b + y_2 + y_1)/(\varphi^{y_2 y_1}(x_2 + (-1)^{y_2} x_1),$$
$$, y_2 + y_1)$$
$$= (\varphi^{(y_2+y_1)(b+y_2+y_1+1)}(\varphi^{by_1+y_1 y_2}(\varphi^{by_2}(a + (-1)^{b} x_2) + (-1)^{b+y_2} x_1))+$$

$$
\begin{aligned}
&+(-1)^{b+y_2+y_1-y_2-y_1+1}\varphi^{y_2y_1}(x_2+(-1)^{y_2}x_1),b)\\
&=(\varphi^{y_2b+y_2+y_2y_1+y_2+y_1b+y_1y_2+y_1+y_1}(\varphi^{by_1+y_1y_2}(\varphi^{by_2}(a+(-1)^bx_2)+(-1)^{b+y_2}x_1))+\\
&+(-1)^{b+1}\varphi^{y_2y_1}(x_2+(-1)^{y_2}x_1),b)\\
&=(\varphi^{y_2b+y_1b}(\varphi^{by_1+y_1y_2}(\varphi^{by_2}(a+(-1)^bx_2)+(-1)^{b+y_2}x_1))+\\
&+(-1)^{b+1}\varphi^{y_2y_1}(x_2+(-1)^{y_2}x_1),b)\\
&=(\varphi^{y_2b+y_1b+y_1b+y_1y_2+by_2}(a+(-1)^bx_2)+(-1)^{b+y_2}\varphi^{y_2b+y_1b+y_1b+y_1y_2}(x_1)+\\
&+(-1)^{b+1}\varphi^{y_1y_2}(x_2+(-1)^{y_2}x_1),b)\\
&=(\varphi^{y_1y_2}(a)+(-1)^b\varphi^{y_1y_2}(x_2)+(-1)^{b+y_2}\varphi^{y_2b+y_1y_2}(x_1)+(-1)^{b+1}\varphi^{y_1y_2}(x_2)+\\
&+(-1)^{b+1+y_2}\varphi^{y_1y_2}(x_1),b)\\
&=(\varphi^{y_1y_2}(a)+(-1)^{b+y_2}\varphi^{y_1y_2}(\varphi^{y_2b}(x_1)-x_1),b).
\end{aligned}
$$

It follows that (4.12), (4.14), (4.16), and (4.18) are then special cases of this equation. We calculate (4.13) by induction on x_1, noting that the case where $x_1 = 1$ is given by (4.12). Suppose the equality holds for all positive integers less than x_1. Then

$$
\begin{aligned}
R^{x_1}_{\mathbf{x},(x_2,y_2)}(a,b) &= R^{x_1-1}_{\mathbf{x},(x_2,y_2)}R_{\mathbf{x},(x_2,y_2)}(a,b)\\
&= R^{x_1-1}_{\mathbf{x},(x_2,y_2)}((-1)^{b+y_2}(\varphi^{by_2}(1)-1)+a,b)\\
&= ((-1)^{b+y_2}(\varphi^{by_2}(1)-1)(x_1-1)+(-1)^{b+y_2}(\varphi^{by_2}(1)-1)+a,b)\\
&= ((-1)^{b+y_2}(\varphi^{by_2}(1)-1)x_1+a,b).
\end{aligned}
$$

Then (4.15) is a special case of (4.13).

Similarly, we calculate (4.17) by induction on y_1. The case where $y_1 = 1$ is (4.16), so suppose the the equality holds for all positive integers less than y_1. Then

$$R^{y_1}_{\mathbf{y},(x_2,y_2)}(a,b) = R^{y_1-1}_{\mathbf{y},(x_2,y_2)}R_{\mathbf{y},(x_2,y_2)}(a,b)$$

$$
\begin{aligned}
&= R^{y_1-1}_{\mathbf{y},(x_2,y_2)}(\varphi^{y_2}(a), b)\\
&= (\varphi^{(y_1-1)y_2}(\varphi^{y_2}(a)), b)\\
&= (\varphi^{y_1y_2}(a), b).
\end{aligned}
$$

Lastly, (4.19) is a special case of (4.17). □

While the equivalence classes were not explicitly used in the last proof, we present here the necessary and sufficient conditions for when two equivalence classes are equal in any quaternionic automorphic loop.

Lemma 4.9. For any quaternionic automorphic loop $Q^{\varphi}_{2^n}$, $\overline{(a,b)} = \overline{(c,d)}$ if and only if either ($a = c$ and $b = d$) or ($c = a + 2^{n-2}$ and $d = b + 2$).

Proof. Suppose first that $\overline{(a,b)} = \overline{(c,d)}$. Then it follows that $\{(a,b), (a,b)(2^{n-2}, 2)\} = \{(c,d), (c,d)(2^{n-2}, 2)\}$, so either $(a,b) = (c,d)$ or $(a,b)(2^{n-2}, 2) = (c,d)$. The latter implies $(\varphi^{2b}(a + (-1)^b 2^{n-2}), b + 2) = (c,d)$. Since $|\varphi| = 2$, this holds if and only if $c = a+(-1)^b 2^{n-2} = a+2^{n-2}$ and $d = b+2$. Thus, either ($a = c$ and $b = d$) or ($c = a+2^{n-2}$ and $d = b + 2$). Alternatively, suppose that $a = c$ and $b = d$. Then it is immediate that $\overline{(a,b)} = \overline{(c,d)}$. In addition, if $c = a + 2^{n-2}$ and $d = b + 2$ then $(c,d) = (a,b)(2^{n-2}, 2)$, so $(c,d) \in \overline{(a,b)}$. Since $(2^{n-2}, 2)$ has order 2 in D, $(c,d) = (a,b)(2^{n-2}, 2)$ if and only if $(c,d)(2^{n-2}, 2) = (a,b)$, so we also have that $(a,b) \in \overline{(c,d)}$ and the equality of equivalence classes follows. □

We will use this fact also without reference when discussing equality. Specifically, we note that the above lemma implies if $\overline{(a,b)} = \overline{(c,b)}$ then it must be true that $a = c$. That is, we will reduce many questions of equality of equivalence classes to a question of equality of coordinates if the second coordinates are equal.

Since we are working in a nonassociative structure, it will be useful to have a condition for when three elements of a quaternionic automorphic loop associate.

Lemma 4.10. Let $Q = Q^{\varphi}_{2^n}$ be a quaternionic automorphic loop of order 2^n and let $\overline{(a,l)}\,, \overline{(b,m)}\,, \overline{(c,p)} \in Q$. Then $\overline{(a,l)} \cdot \overline{(b,m)(c,p)} = \overline{(a,l)(b,m)} \cdot \overline{(c,p)}$ if and only if

$$\varphi^{lm}(a) + (-1)^{m+l}\varphi^{lm+mp}(c) = \varphi^{mp+lm}(a) + (-1)^{m+l}\varphi^{mp}(c). \tag{4.20}$$

Proof. Using the results from Lemma 4.9 we calculate to get:

$$\begin{aligned}
&\overline{(a,l)} \cdot \overline{(b,m)(c,p)} = \overline{(a,l)(b,m)} \cdot \overline{(c,p)} \\
&\Leftrightarrow \overline{(\varphi^{l(m+p)}(a + (-1)^l\varphi^{mp}(b + (-1)^m c)), l + m + p)} \\
&\quad = \overline{(\varphi^{(l+m)p}(\varphi^{lm}(a + (-1)^l b) + (-1)^{l+m}c), l + m + p)} \\
&\Leftrightarrow \varphi^{lm+lp}(a) + (-1)^l\varphi^{mp+lm+lp}(b) + (-1)^{m+l}\varphi^{mp+lm+lp}(c) \\
&\quad = \varphi^{lp+mp+lm}(a) + (-1)^l\varphi^{lp+mp+lm}(b) + (-1)^{l+m}\varphi^{lp+mp}(c) \\
&\Leftrightarrow \varphi^{lm+lp}(a) + (-1)^{m+l}\varphi^{mp+lm+lp}(c) = \varphi^{lp+mp+lm}(a) + (-1)^{l+m}\varphi^{lp+mp}(c) \\
&\Leftrightarrow \varphi^{lm}(a) + (-1)^{m+l}\varphi^{lm+mp}(c) = \varphi^{mp+lm}(a) + (-1)^{m+l}\varphi^{mp}(c).
\end{aligned}$$

□

4.4 The quaternionic automorphic loop of order 8

To give the reader an idea of the structure of the quaternionic automorphic loops, we present here the example of order 8. While there are three distinct quaternionic automorphic loops of order 2^n for $n > 3$, the three automorphisms collapse when $n = 3$. More specifically, in the order 8 case, $\alpha = 2^{n-2} - 1 = 1$, $\beta = 2^{n-2} + 1 = 3$, and $\iota = -1$. The first coordinate is taken modulo $2^{n-1} = 4$. So α is the identity (making $Q^{\alpha}_8 \cong Q_8$, the quaternion group) and $\beta = \iota = -1$.

The following are the equivalence classes of Q^{ι}_8, labeled in a way which mimics the quaternion group of order 8:

$$\begin{array}{llll}
\langle(2,2)\rangle = \{(0,0),(2,2)\} & \to 1 & \overline{(0,2)} = \{(0,2),(2,0)\} & \to -1 \\
\overline{(1,0)} = \{(3,2),(1,0)\} & \to i & \overline{(1,2)} = \{(1,2),(3,0)\} & \to -i \\
\overline{(0,1)} = \{(0,1),(2,3)\} & \to j & \overline{(0,3)} = \{(0,3),(2,1)\} & \to -j \\
\overline{(1,1)} = \{(1,1),(3,3)\} & \to k & \overline{(1,3)} = \{(1,3),(3,1)\} & \to -k
\end{array}$$

Then the multiplication table of Q_8^ι is:

$\cdot$	1	-1	i	j	k	$-i$	$-j$	$-k$
1	1	-1	i	j	k	$-i$	$-j$	$-k$
-1	-1	1	$-i$	$-j$	$-k$	i	j	k
i	i	$-i$	-1	k	$-j$	1	$-k$	j
j	j	$-j$	$-k$	-1	$-i$	k	1	i
k	k	$-k$	j	i	-1	$-j$	$-i$	1
$-i$	$-i$	i	1	$-k$	j	-1	k	$-j$
$-j$	$-j$	j	k	1	i	$-k$	-1	$-i$
$-k$	$-k$	k	$-j$	$-i$	1	j	i	-1

Notice first that there is a unique element of order 2: $-1 = \overline{(0,2)}$, and that every element $a \notin \{1,-1\}$ squares to this -1. This is a property of the quaternion group of order 8 as well, and we will show in §4.5 that this holds in a general way for the quaternionic automorphic loops of higher orders. We also note that the element -1 is in the center, as it is in the group case, and we will show that it is the only non-identity element in the center for all quaternionic loops. Lastly, we note here that Q_8^ι is, indeed, non-associative. Take, for example: $ij \cdot k = -1$ and $i \cdot jk = 1$.

4.5 Main results

There are many properties of quaternionic automorphic loops which are reminiscent of their group analogs. While the three quaternionic automorphic loops of a certain order share many of these properties such as being 2-generated, having a unique element of order 2, having a 2-element center, and others, there are some quaternion group-like properties which are disbursed between the three, and other properties which come strictly from nonassociativity. This section will act as an exposition of these loops with a collection of results that is by no means exhaustive, but hopefully acts as a first attempt to understand their structure.

Proposition 4.11. Let D be the dihedral-like loop of order 2^{n+1} constructed in Section 4.2. Then D is generated by $x = (1,0)$ and $y = (0,1)$. Specifically, for $(a,b) \in D$, $(a,b) = x^a y^b$. Consequently, $Q_{2^n}^{\varphi}$ is generated by $\mathbf{x} = \overline{(1,0)}$ and $\mathbf{y} = \overline{(0,1)}$ and $\overline{(a,b)} = \mathbf{x}^a\mathbf{y}^b$.

Proof. Let $(a,b) \in D$ and consider $(1,0)^a = (1,0)\cdots(1,0)$. It is our goal to show $(1,0)^a = (a,0)$. We proceed by induction on a. The case where $a = 1$ holds, as certainly $(1,0) = (1,0)$. Now suppose $(1,0)^u = (u,0)$ for every $u < a$. Then, since automorphic loops are power-associative:

$$\begin{aligned}
(1,0)^a &= (1,0)^{a-1}(1,0) \\
&= (a-1,0)(1,0) \\
&= (\varphi^0(a-1+(-1)^0 1),0) \\
&= (a,0).
\end{aligned}$$

Now consider $(0,1)^b$. It is our goal to show $(0,1)^b = (0,b)$. We proceed by induction on b. The case where $b = 1$ holds trivially, so suppose that $(0,1)^u = (0,u)$ for every $u < b$. Again, since automorphic loops are power-associative, we have:

$$\begin{aligned}
(0,1)^b &= (0,1)^{b-1}(0,1) \\
&= (0,b-1)(0,1) \\
&= (\varphi^{b-1}(0+(-1)^{b-1}0), b-1+1) \\
&= (0,b).
\end{aligned}$$

Thus, $x^a y^b = (1,0)^a(0,1)^b = (a,0)(0,b) = (\varphi^0(a + (-1)^0 0), 0 + b) = (a,b)$, so x and y generate D, as desired. It then follows immediately that for any $\overline{(a,b)} \in Q^{\varphi}_{2^n}$, $\overline{(a,b)} = \mathbf{x}^a\mathbf{y}^b$ as well. □

Since the first coordinate is taken modulo $\mathbb{Z}_{2^{n-1}}$ and the second coordinate modulo $\mathbb{Z}_4$, the following is a direct result of Proposition 4.11.

Corollary 4.12. In any $Q^{\varphi}_{2^n}$, $\mathbf{x}$ has order 2^{n-1} and $\mathbf{y}$ has order 4.

The following properties are analogs to the properties found in the generalized quaternion groups which were listed in Theorem 4.5.

Lemma 4.13. Let $Q = Q^{\varphi}_{2^n}$. Then:

(a) $\mathbf{x}^{2^{n-2}} = \mathbf{y}^2$ in Q

(b) Every element of Q can be written in the form $\mathbf{x}^a$ or $\mathbf{x}^a\mathbf{y}$ for some $a \in \mathbb{Z}$.

(c) Every element g of Q outside of $\langle \mathbf{x} \rangle$ has order 4 and $g^2 = \mathbf{y}^2$.

(d) The element $\mathbf{x}^{2^{n-2}} = \mathbf{y}^2 = \overline{(0,2)}$ of Q is the unique element of order 2.

(e) For each $g \in Q$ such that $g \notin \langle \mathbf{x} \rangle$, $T_g(\mathbf{x}) = \mathbf{x}^{-1}$.

Proof. For (a), notice

$$(2^{n-2}, 0)(2^{n-2}, 2) = (\varphi^0(2^{n-2} + (-1)^0 \cdot 2^{n-2}), 0 + 2) = (0, 2),$$

so

$$\mathbf{x}^{2^{n-2}} = \overline{(2^{n-2}, 0)} = \overline{(0,2)} = \mathbf{y}^2.$$

For (b), Proposition 4.11 gives that every element can be written in the form $\mathbf{x}^a\mathbf{y}^b$ for some $a, b \in \mathbb{Z}$. By (a), we have that even powers of $\mathbf{y}$ can be written as powers of $\mathbf{x}$. Thus, for b even, the result follows from Lemma 4.1. If b is odd, then $b = 1$ or $b = 3$. However,

$$(a, 3)(2^{n-2}, 2) = (\varphi^6(a + (-1)^3 \cdot 2^{n-2}), 1) = (a - 2^{n-2}, 1)$$

so $\overline{(a, 3)} = \overline{(a', 1)}$ for some $a' \in \mathbb{Z}_{2^{n-1}}$. Thus, $\mathbf{x}^a\mathbf{y}^b = \mathbf{x}^{a'}\mathbf{y}$ in this case and the result follows.

For (c), let $g \in Q$ such that $g \notin \langle \mathbf{x} \rangle$. Then $g = \mathbf{y}$ or $g = \mathbf{x}^a\mathbf{y}$ for some a. We have already shown that $\mathbf{y}$ has order 4 and certainly $\mathbf{y}^2 = \mathbf{y}^2$, so consider $g = \mathbf{x}^a\mathbf{y}$. Then

$$g^2 = (\mathbf{x}^a\mathbf{y})^2 = \overline{(a, 1)} \cdot \overline{(a, 1)} = \overline{(\varphi(a + (-1)a), 2)} = \overline{(0, 2)} = \mathbf{y}^2.$$

Since $\mathbf{y}$ has order 4, $\mathbf{y}^2$ has order 2. Thus, g^2 has order 2, implying that g has order 4.

For (d), we see that by (c), every element which is not a power of $\mathbf{x}$ has order 4, thus, any element with order 2 must be a power of $\mathbf{x}$. However, the only element of $\langle \mathbf{x} \rangle$ with order 2 is $\mathbf{x}^{2^{n-2}}$, as desired.

For (e), we see that by (b), any element g outside of $\langle \mathbf{x} \rangle$ has form $g = \mathbf{x}^a\mathbf{y}$ for some a. Then $T_g(\mathbf{x}) = T_{\overline{(a,1)}}\overline{(1, 0)} = \overline{((1 + (-1)^{0+1})a + (-1)^1 1, 0)} = \overline{(-1, 0)} = \mathbf{x}^{-1}$, as desired. □

Corollary 4.14. Let $Q = Q_{2^n}^{\varphi}$ and $1 \neq H \leq Q$. Then $\langle \mathbf{x}^{2^{n-2}} \rangle \leq H$.

Proof. From the above argument, we may conclude that for any $1 \neq H \leq Q$ such that $g = \mathbf{x}^a\mathbf{y} \in H \not\subset \langle \mathbf{x} \rangle$, $g^2 = \mathbf{y}^2 = \mathbf{x}^{2^{n-2}} \in H$. Suppose then that $1 \neq H \leq \langle \mathbf{x} \rangle$. This means H is cyclic of even order, and hence contains an element of order 2, which must be $\mathbf{x}^{2^{n-2}}$ by Lemma 4.13(d). □

Corollary 4.15. Quaternionic automorphic loops cannot be constructed from a semidirect product.

Proof. By Corollary 4.14, no two proper, nontrivial subloops have trivial intersection, and so Q cannot be constructed from a loop semidirect product. □

4.5.1 Nuclei and Center.

Proposition 4.16. For $Q = Q^{\varphi}_{2^n}$, the middle nucleus of Q is isomorphic to $\mathbb{Z}_{2^{n-1}}$ and generated by $\mathbf{x}$.

Proof. Let $\overline{(b,m)} \in Q$. Then $\overline{(b,m)} \in N_\mu(Q)$ if and only if for every $\overline{(a,l)}\,,\overline{(c,p)} \in Q$,

$$\overline{(a,l)(b,m)} \cdot \overline{(c,p)} = \overline{(a,l)} \cdot \overline{(b,m)(c,p)}\,.$$

From Lemma 4.10, this holds if and only if (4.20) holds for every $\overline{(a,l)}\,,\overline{(c,p)} \in Q$:

$$\varphi^{lm}(a) + (-1)^{m+l}\varphi^{lm+mp}(c) = \varphi^{mp+lm}(a) + (-1)^{m+l}\varphi^{mp}(c)\,.$$

It is clear that, being the neutral element, $\overline{(0,0)} \in N_\mu(Q)$. Moreover, we note that (4.20) does not depend on b. Thus, $\langle \mathbf{x} \rangle \le N_\mu(Q)$.

Now to see that there are no other elements besides powers of $\mathbf{x}$, suppose $\overline{(b,m)} \in N_\mu(Q)$. Then (4.20) holds for every $\overline{(a,l)}\,,\overline{(c,p)} \in Q$, so take $(a,l) = (0,1)$ and $(c,p) = (c,0)$ in particular. Then $\overline{(b,m)} \in N_\mu(Q)$ implies that

$$0 + (-1)^{1+m}\varphi^m(c) = 0 + (-1)^{m+1}c.$$

Simplifying, this gives

$$\varphi^m(c) = c.$$

Since φ is not the identity, it follows that if $\overline{(b,m)} \in N_\mu(Q)$ then $m = 0$ or $m = 2$.

However,

$$(b,2)(2^{n-2},2) = (\varphi^4(b + (-1)^2 \cdot 2^{n-2}), 4) = (b + 2^{n-2}, 0).$$

So $\overline{(b,2)} = \overline{(d,0)}$ for some $\overline{(d,0)} \in Q$. Thus, $\overline{(b,m)} \in N_\mu(Q)$ if and only if $m = 0$. That is, $N_\mu(Q) = \langle \mathbf{x} \rangle \cong \mathbb{Z}_{2^{n-1}}$. □

While all three quaternionic automorphic loops of the same order share the same middle nucleus, there is some distinction in their left nuclei, as detailed by the following lemmas.

Lemma 4.17. For $Q = Q^{\varphi}_{2^n}$, if $\overline{(a,l)} \in N_\lambda(Q)$ then $a = \varphi(a)$ and $l \in \{0,2\}$.

Proof. Let $\overline{(a,l)} \in Q^{\varphi}_{2^n}$. Then $\overline{(a,l)} \in N_\lambda(Q^{\varphi}_{2^n})$ if and only if for every $\overline{(b,m)}\,, \overline{(c,p)} \in Q^{\varphi}_{2^n}$,

$$\overline{(a,l)(b,m)} \cdot \overline{(c,p)} = \overline{(a,l)} \cdot \overline{(b,m)(c,p)}\,.$$

We again remind the reader of the associativity condition from (4.20), so the above is equivalent to the following for every $\overline{(b,m)}\,, \overline{(c,p)} \in Q^{\varphi}_{2^n}$:

$$\varphi^{lm}(a) + (-1)^{m+l}\varphi^{lm+mp}(c) = \varphi^{mp+lm}(a) + (-1)^{m+l}\varphi^{mp}(c)\,.$$

If $\overline{(a,l)} \in N_\lambda(Q^{\varphi}_{2^n})$, then (4.20) must hold for any choice of $\overline{(b,m)}$ and $\overline{(c,p)}$, so let $c = 0$ and $m = p = 1$. Then the associativity condition reduces to $\varphi^l(a) = \varphi^{l+1}(a)$, or

$$a = \varphi(a)\,.$$

Moreover, by letting $c = m = 1$ and $p = 0$ in (4.20), the associativity condition becomes $\varphi^l(a) + (-1)^{1+l}\varphi^l(1) = \varphi^l(a) + (-1)^{l+1} \cdot 1$ which reduces to

$$\varphi^l(1) = 1\,.$$

Since $\varphi \neq \mathrm{id}$, it follows that l is even. However, l is taken modulo 4, so $l = 0$ or $l = 2$. □

Lemma 4.18. $N_\lambda(Q^\iota_{2^n}) = \langle \mathbf{x}^{2^{n-2}} \rangle \cong \mathbb{Z}_2$.

Proof. We first calculate using (4.20) with $(a, l) = (2^{n-2}, 0)$ and $\varphi = \iota = -1$ to see that $\mathbf{x}^{2^{n-2}} \in N_\lambda(Q^\iota_{2^n})$ if and only if for every $\overline{(b, m)}, \overline{(c, p)} \in Q^\iota_{2^n}$:

$$\begin{aligned} (-1)^0(2^{n-2}) + (-1)^m(-1)^{mp}(c) &= (-1)^{mp}(2^{n-2}) + (-1)^m(-1)^{mp}c \\ \Leftrightarrow \quad 2^{n-2} &= (-1)^{mp}2^{n-2}. \end{aligned}$$

Since $2^{n-2} = -2^{n-2} \mod 2^{n-1}$, the equation above is an identity, so $\mathbf{x}^{2^{n-2}} \in N_\lambda(Q^\iota_{2^n})$.

Now Lemma 4.17 with $\varphi = \iota = -1$ implies that if $\overline{(a, l)} \in N_\lambda(Q^\iota_{2^n})$, then $a = -a$. This only holds for $a = 0$ or $a = 2^{n-2}$. Moreover, Lemma 4.17 also gives that if $\overline{(a, l)} \in N_\lambda(Q^\iota_{2^n})$ then $l = 0$ or $l = 2$. However, $\overline{(a, 0)} = \overline{(a', 2)}$ for some a', so it follows that if $\overline{(a, l)} \in N_\lambda(Q^\iota_{2^n})$, then $\overline{(a, l)} \in \{\overline{(0, 0)}, \overline{(2^{n-2}, 0)}\} = \langle \mathbf{x}^{2^{n-2}} \rangle$.

Lastly, the map from $\langle \mathbf{x}^{2^{n-2}} \rangle \to \mathbb{Z}_2$ sending $\mathbf{x}^{2^{n-2}} \mapsto 1$ gives the desired isomorphism.

□

Lemma 4.19. $N_\lambda(Q^\alpha_{2^n}) = \langle \mathbf{x}^{2^{n-2}} \rangle \cong \mathbb{Z}_2$.

Proof. Again, we use (4.20) with $(a, l) = (2^{n-2}, 0)$ and $\varphi = \alpha$ to see that $\mathbf{x}^{2^{n-2}} \in N_\lambda(Q^\alpha_{2^n})$ if and only if for every $\overline{(b, m)}, \overline{(c, p)} \in Q^\alpha_{2^n}$:

$$\alpha^0(2^{n-2}) + (-1)^m\alpha^{mp}(c) = \alpha^{mp}(2^{n-2}) + (-1)^m\alpha^{mp}(c)$$

$$\Leftrightarrow \quad 2^{n-2} = \alpha^{mp}(2^{n-2}).$$

If mp is even, then the result follows immediately, so suppose mp is odd. From Lemma 4.7 we have that α acts as negation on even inputs, so the equation above is equivalent to saying $2^{n-2} = -2^{n-2}$, which holds. Thus, $\mathbf{x}^{2^{n-2}} \in N_\lambda(Q^\alpha_{2^n})$.

Now Lemma 4.17 with $\varphi = \alpha = 2^{n-2} - 1$ implies that if $\overline{(a,l)} \in N_\lambda(Q^\alpha_{2^n})$, then $a = (2^{n-2} - 1)a$, or $a = 2^{n-2}a - a$, or again equivalently $a(2^{n-2} - 2) = 0$. The only solutions to this equation in $\mathbb{Z}_{2^{n-1}}$ are $a = 0$ or $a = 2^{n-2}$. Moreover, in a similar way to Lemma 4.18, we have that $l = 0$, so $N_\lambda(Q^\alpha_{2^n}) = \langle \mathbf{x}^{2^{n-2}} \rangle$ as well, and the same map as above will give the desired isomorphism. □

Lemma 4.20. $N_\lambda(Q^\beta_{2^n}) = \langle \mathbf{x}^2 \rangle \cong \mathbb{Z}_{2^{n-2}}$.

Proof. Here we use (4.20) with $(a,l) = (2,0)$ and $\varphi = \beta = 2^{n-2} + 1$ to see that $\mathbf{x}^2 \in N_\lambda(Q^\beta_{2^n})$ if and only if for every $\overline{(b,m)}, \overline{(c,p)} \in Q^\beta_{2^n}$:

$$\beta^0 2 + (-1)^m \beta^{mp}(c) = \beta^{mp}(2) + (-1)^m \beta^{mp}(c)$$
$$\Leftrightarrow \quad 2 = \beta^{mp}(2).$$

From Lemma 4.7, we have that β acts as the identity on even inputs, so the above holds giving that $\mathbf{x}^2 \in N_\lambda(Q^\beta_{2^n})$.

Now Lemma 4.17 with $\varphi = \beta$ implies that if $\overline{(a,l)} \in N_\lambda(Q^\beta_{2^n})$, then $a = \beta(a)$. Since β only acts as the identity on even inputs, it follows that a must be even. By Lemma 4.17, $l = 0$, so $N_\lambda(Q^\beta_{2^n}) = \langle \mathbf{x}^2 \rangle$.

The map from $\langle \mathbf{x}^2 \rangle \to \mathbb{Z}_{2^{n-2}}$ sending $\mathbf{x}^2 \mapsto 1$ gives the desired isomorphism. □

Lemma 4.21. For $Q = Q^\varphi_{2^n}$, $C(Q) = \langle \mathbf{x}^{2^{n-2}} \rangle$ and $C(Q) \cong \mathbb{Z}_2$.

Proof. By Lemma 4.13, we see that $\overline{(0,2)} = \mathbf{x}^{2^{n-2}} = \mathbf{y}^2$ is the unique element of Q of order 2, thus it must be preserved by all inner mappings. In particular, $T_a(\mathbf{x}^{2^{n-2}}) = \mathbf{x}^{2^{n-2}}$ for every $a \in Q$, so $\mathbf{x}^{2^{n-2}} \in C(Q)$.

To see that $\overline{(0,2)}$ is the only non-identity element in the commutant, we calculate the following. For $\overline{(a,b)} \in Q$, $\overline{(a,b)} \in C(Q)$ if and only if $\overline{(x,y)} \cdot \overline{(a,b)} = \overline{(a,b)} \cdot \overline{(x,y)}$ for every $\overline{(x,y)} \in Q$, or equivalently, $\overline{(\varphi^{yb}(x+(-1)^y a), y+b)} = \overline{(\varphi^{by}(a+(-1)^b x), b+y)}$. This identity holds if and only if for every $x \in \mathbb{Z}_{2^{n-1}}$ and for every $y \in \mathbb{Z}_4$,

$$x + (-1)^y a = a + (-1)^b x. \qquad (*)$$

Letting $y = 0$ in $(*)$ yields $x + a = a + (-1)^b x$ or $x = (-1)^b x$. This implies that if $\overline{(a,b)} \in C(Q)$, then $b = 0$ or $b = 2$.

Moreover, letting $x = 0$ and $y = 1$ in $(*)$ yields $-a = a$, which implies that if $\overline{(a,b)} \in C(Q)$, then $a = 0$ or $a = 2^{n-2}$. Thus, $(a,b) \in \{(0,0),(0,2),(2^{n-2},0),(2^{n-2},2)\}$. Noticing that $\{(0,0),(2^{n-2},2)\} = \overline{(0,0)}$ and $\{(0,2),(2^{n-2},0)\} = \overline{(0,2)}$, it follows that the commutant of Q is equal to $C(Q) := \{\overline{(0,0)}, \mathbf{x}^{2^{n-2}}\} = \langle \mathbf{x}^{2^{n-2}} \rangle \cong \mathbb{Z}_2$, as desired. □

Proposition 4.22. For $Q = Q_{2^n}^{\varphi}$, $Z(Q) = \langle \mathbf{x}^{2^{n-2}} \rangle$ and $Z(Q) \cong \mathbb{Z}_2$.

Proof. By Lemma 4.13 again, $\mathbf{x}^{2^{n-2}}$ is the unique element of Q of order 2, thus it must be preserved by all inner mappings. This shows that $\mathbf{x}^{2^{n-2}} \in Z(Q)$. Since $Z(Q) = C(Q) \cap N(Q)$, Lemma 4.21 gives us that $C(Q) = Z(Q) = \langle \mathbf{x}^{2^{n-2}} \rangle$. □

This proposition in combination with Corollary 4.14 shows that the pairwise intersection of two nontrivial subloops contains the center of the loop, a fact which we make explicit in the following corollary. This is also the case in the generalized quaternion groups.

Corollary 4.23. For $Q = Q_{2^n}^{\varphi}$ and any two nontrivial subloops $H, K \le Q$, $Z(Q) \le H \cap K = \langle \mathbf{x}^{2^{n-2}} \rangle$.

4.5.2 Inner mapping groups.

Lemma 4.24. For $Q = Q_{2^n}^{\varphi}$, $\mathrm{RInn}(Q) = \langle R_{\mathbf{y},\overline{(x_2,y_2)}}, R_{\mathbf{x},\overline{(x_2,y_2)}} : \overline{(x_2,y_2)} \in Q\rangle$. In fact, $R^{y_1}_{\mathbf{y},\overline{(x_2,y_2)}} R^{x_1}_{\mathbf{x},\overline{(x_2,y_2)}} = R_{\overline{(x_1,y_1)},\overline{(x_2,y_2)}}$.

Proof. Recall $\mathrm{RInn}(Q) = \langle R_{u,v} : u, v \in Q\rangle$. Let $x_1, y_1, x_2, y_2, a, b \in Q$. It suffices to show that the generator of $\mathrm{RInn}(Q)$, $R_{\overline{(x_1,y_1)},\overline{(x_2,y_2)}}$ can be written as a composition of powers of $R_{\mathbf{y},\overline{(x_2,y_2)}}$ and $R_{\mathbf{x},\overline{(x_2,y_2)}}$. Recall, from (4.11):

$$R_{(x_1,y_1),(x_2,y_2)}(a,b) = ((-1)^{b+y_2}\varphi^{y_2y_1}(\varphi^{by_2}(x_1) - x_1) + \varphi^{y_2y_1}(a), b).$$

Now using (4.13) and (4.17), we have:

$$\begin{aligned}
R^{y_1}_{\mathbf{y},(x_2,y_2)} R^{x_1}_{\mathbf{x},(x_2,y_2)}(a,b) &= R^{y_1}_{\mathbf{y},(x_2,y_2)}((-1)^{b+y_2}(\varphi^{by_2}(x_1) - x_1) + a, b) \\
&= (\varphi^{y_1y_2}((-1)^{b+y_2}(\varphi^{by_2}(x_1) - x_1) + a), b) \\
&= ((-1)^{b+y_2}\varphi^{y_1y_2}(\varphi^{by_2}(x_1) - x_1) + \varphi^{y_1y_2}(a), b) \\
&= R_{(x_1,y_1),(x_2,y_2)}(a,b).
\end{aligned}$$

Thus, $R_{\mathbf{y},\overline{(x_2,y_2)}}$ and $R_{\mathbf{x},\overline{(x_2,y_2)}}$ generate $\mathrm{RInn}(Q)$. □

Lemma 4.25. Recall $\mathbf{z} = \overline{(1,1)}$. In $Q_{2^n}^{\varphi}$, $R_{\mathbf{x},(x_2,y_2)} = R_{\mathbf{x},\mathbf{z}}^{(y_2 \mod 2)}$ and $R_{\mathbf{y},(x_2,y_2)} = R_{\mathbf{y},\mathbf{z}}^{y_2}$.

Proof. That $R_{\mathbf{y},(x_2,y_2)} = R_{\mathbf{y},\mathbf{z}}^{y_2}$ follows immediately from (4.19) and (4.16). Now,

$$R_{\mathbf{x},\mathbf{z}}^{(y_2 \mod 2)}(a,b) = ((-1)^{b+1}(\varphi^{b}(1) - 1)(y_2 \mod 2) + a, b)$$

and

$$R_{\mathbf{x},(x_2,y_2)}(a,b) = ((-1)^{b+y_2}(\varphi^{by_2}(1) - 1) + a, b).$$

For y_2 even we have

$$R_{\mathbf{x},\mathbf{z}}^{(y_2 \mod 2)}(a,b) = (a,b) = R_{\mathbf{x},(x_2,y_2)}(a,b).$$

For y_2 odd, we have

$$R_{\mathbf{x},\mathbf{z}}^{(y_2 \mod 2)}(a,b) = ((-1)^{b+1}(\varphi^b(1)-1)+a,b) = R_{\mathbf{x},(x_2,y_2)}(a,b).$$

Therefore, $R_{\mathbf{x},(x_2,y_2)} = R_{\mathbf{x},\mathbf{z}}^{(y_2 \mod 2)}$, as desired. □

Lemma 4.24 can thus be rewritten using these new generators as follows.

Corollary 4.26. For $Q = Q_{2^n}^{\varphi}$,

$$\mathrm{RInn}(Q) = \langle R_{\mathbf{x},\mathbf{z}}, R_{\mathbf{y},\mathbf{z}} \rangle.$$

Proposition 4.27. For $Q = Q_{2^n}^{\varphi}$, let $s := T_{\mathbf{y}}$ and $r := T_{\mathbf{x}}$. Then $s^2 = r^{2^{n-2}} = 1$, $srs^{-1} = r^{-1}$, and $\langle s, r \rangle = \mathrm{MInn}(Q)$. In particular, $T_{\overline{(u,v)}} = T_{\mathbf{x}}^u T_{\mathbf{y}}^v$ for $\overline{(u,v)} \in Q$.

Proof. Recall $T_{\mathbf{y}}(a,b) = (-a,b)$, so $T_{\mathbf{y}}$ maps the first coordinate of an ordered pair to its inverse. This clearly has order 2. Moreover, recall $T_{\mathbf{x}}(a,b) = (1+(-1)^{b+1}+a,b)$. For b even, this reduces to (a,b), and for b odd, this reduces to $(2+a,b)$.

When b is even, $T_{\mathbf{x}}$ is the identity map, in which case all the identities in the proposition hold trivially. So suppose b is odd. Then $T_{\mathbf{x}}^u(a,b) = (2u+a,b)$. Since the first coordinate is taken modulo 2^{n-1}, $\overline{(2u+a,b)} = \overline{(a,b)}$ whenever $u \equiv 0$ or $u \equiv 2^{n-2}$. Thus, r has order 2^{n-2}.

To show $srs^{-1} = r^{-1}$, it suffices to show $srs = r^{-1}$, so we calculate, making use of (4.5), (4.6), and (4.7):

$$\begin{aligned} T_{\mathbf{y}}T_{\mathbf{x}}T_{\mathbf{y}}(a,b) &= T_{\mathbf{y}}T_{\mathbf{x}}(-a,b) \\ &= T_{\mathbf{y}}(1+(-1)^{b+1}-a,b) \\ &= (-(1+(-1)^{b+1}-a),b) \\ &= (-1+(-1)^{b}+a,b) \\ &= T_{\mathbf{x}}^{-1}(a,b). \end{aligned}$$

Lastly, we show that s and r generate $\mathrm{MInn}(Q)$. It suffices to show that

$$T_{(u,v)}(a,b) = T_{\mathbf{x}}^{u}T_{\mathbf{y}}^{v}(a,b).$$

Calculating using (4.4), (4.6), and (4.8) it follows immediately:

$$T_{\mathbf{x}}^{u}T_{\mathbf{y}}^{v}(a,b) = T_{\mathbf{x}}^{u}((-1)^{v}a,b) = ((1+(-1)^{b+1})u+(-1)^{v}a,b) = T_{(u,v)}(a,b).$$

□

Corollary 4.28. $\mathrm{MInn}(Q_{2^n}^{\varphi}) \cong D_{2^{n-1}}$.

Theorem 4.29. For $Q = Q_{2^n}^{\iota}$, $\mathrm{Inn}(Q) \cong D_{2^{n-1}}$.

Proof. By Lemma 4.3, it suffices to show that $\mathrm{RInn}(Q) = \mathrm{MInn}(Q)$, that is, that the generators of one can be written in terms of the generators of the other. We start with:

$$R_{\mathbf{x},\mathbf{z}}(a,b) = ((-1)^{b+1}((-1)^{b}-1)+a,b) = ((-1)+(-1)^{b}+a,b) = T_{\mathbf{x}}^{-1}(a,b).$$

Moreover,

$$R_{\mathbf{y},\mathbf{z}}(a,b) = ((-1)a,b) = (-a,b) = T_{\mathbf{y}}(a,b).$$

Thus, $\mathrm{LInn}(Q) = \mathrm{RInn}(Q) = \mathrm{MInn}(Q) = \mathrm{Inn}(Q)$. An application of Proposition 4.27 finishes the proof. □

Lemma 4.30. In $Q_{2^n}^{\alpha}$, $R_{\mathbf{x},\mathbf{z}} = T_{\mathbf{x}}^{2^{n-3}-1}$

Proof. In $Q_{2^n}^{\alpha}$, we have that

$$R_{\mathbf{x},\mathbf{z}}(a,b) = ((-1)^{b+1}((2^{n-2}-1)^b - 1) + a, b)$$

and

$$T_{\mathbf{x}}^{2^{n-3}-1}(a,b) = ((1+(-1)^{b+1})(2^{n-3}-1)+a, b).$$

For b odd, the first reduces to $(2^{n-2}-1-1+a,b) = (2^{n-2}-2+a,b)$ and the second simplifies to $(2(2^{n-3}-1)+a,b) = (2^{n-2}-2+a,b)$, as desired. For b even, the first reduces to $((1-1)+a,b) = (a,b)$ and the second becomes $((1-1)(2^{n-3}-1)+a,b) = (a,b)$ as well. Thus, we have equality in all cases. □

Theorem 4.31. $\mathrm{Inn}(Q_{2^n}^{\alpha}) \cong \mathbb{Z}_2 \times D_{2^{n-1}}$.

Proof. Let $H := \langle T_{\mathbf{y}} R_{\mathbf{y},\mathbf{z}} \rangle$ and $K := \langle T_{\mathbf{x}}, T_{\mathbf{y}} \rangle$ be subgroups of $\mathrm{Inn}(Q_{2^n}^{\alpha})$. We have shown in Proposition 4.27 that $T_{\mathbf{x}}$ and $T_{\mathbf{y}}$ generate a group isomorphic to $D_{2^{n-1}}$. We claim now the following:

$$T_{\mathbf{y}} R_{\mathbf{y},\mathbf{z}} = R_{\mathbf{y},\mathbf{z}} T_{\mathbf{y}} \qquad \text{and} \qquad |T_{\mathbf{y}} R_{\mathbf{y},\mathbf{z}}| = 2.$$

To see the first, we calculate

$$T_{\mathbf{y}} R_{\mathbf{y},\mathbf{z}}(a,b) = T_{\mathbf{y}}((2^{n-2}-1)a,b) = (-(2^{n-2}-1)a,b)$$

and also

$$R_{\mathbf{y},\mathbf{z}}T_{\mathbf{y}}(a,b) = R_{\mathbf{y},\mathbf{z}}(-a,b) = ((2^{n-2}-1)(-a),b) = (-(2^{n-2}-1)a,b)\,,$$

as desired. To show $|T_{\mathbf{y}}R_{\mathbf{y},\mathbf{z}}| = 2$, we first note that since $R_{\mathbf{y},\mathbf{z}} = (\alpha(a),b)$ and $|\alpha| = 2$, then $|R_{\mathbf{y},\mathbf{z}}| = 2$. Moreover, since $|T_{\mathbf{y}}| = 2$, it follows that:

$$(T_{\mathbf{y}}R_{\mathbf{y},\mathbf{z}})^2 = T_{\mathbf{y}}^2 R_{\mathbf{y},\mathbf{z}}^2 = 1.$$

Thus, $\langle T_{\mathbf{y}}R_{\mathbf{y},\mathbf{z}}\rangle \cong \mathbb{Z}_2$.

We claim now that $\mathrm{Inn}(Q_{2^n}^{\alpha}) = H \times K$. To see that the intersection of H and K is trivial, let $\gamma \in H \cap K$ and suppose by way of contradiction that $\gamma \neq 1$. Since $|H| = 2$, and $\gamma \in H$, γ then must be equal to $T_{\mathbf{y}}R_{\mathbf{y},\mathbf{z}}$ and so $|\gamma| = 2$. It is well known that the only elements of order 2 in the dihedral group of order 2^{n-1} are the reflections $s, rs, r^2s, \ldots, r^{2^{n-2}-1}s$ and the rotation by π: $r^{2^{n-3}}$. Thus, for $\gamma \in K$, $\gamma = T_{\mathbf{x}}^m T_{\mathbf{y}}$ for some $0 \leq m < 2^{n-2}$ or $\gamma = T_{\mathbf{x}}^{2^{n-3}}$. For the first case, this would imply

$$\begin{aligned} & T_{\mathbf{y}}R_{\mathbf{y},\mathbf{z}} = T_{\mathbf{x}}^m T_{\mathbf{y}} \\ \Leftrightarrow\quad & R_{\mathbf{y},\mathbf{z}}T_{\mathbf{y}} = T_{\mathbf{x}}^m T_{\mathbf{y}} \\ \Leftrightarrow\quad & R_{\mathbf{y},\mathbf{z}} = T_{\mathbf{x}}^m \end{aligned}$$

If $m = 0$, this then implies that $R_{\mathbf{y},\mathbf{z}} = 1$, which is a contradiction since $\alpha \neq 1$. So suppose that $m \neq 0$. Then $R_{\mathbf{y},\mathbf{z}}(\overline{(a,b)}) = T_{\mathbf{x}}^m(\overline{(a,b)})$ implies

$$\overline{(\alpha(a),b)} = \overline{((1+(-1)^{b+1})m+a,b)}.$$

Since the second coordinates are equal, we must then have equality in the first coordinates, so

$$(2^{n-2}-1)a = (1+(-1)^{b+1})m + a.$$

Since this must hold for every $\overline{(a,b)}$, take $b=0$. Then this implies that $(2^{n-2}-1)a = a$ and thus $2^{n-2}-1=1$, which again is a contradiction. So it cannot be the case that $\gamma = T_{\mathbf{x}}^m T_{\mathbf{y}}$.

For the second case, we suppose $\gamma = T_{\mathbf{x}}^{2^{n-3}}$. This implies that $T_{\mathbf{y}}R_{\mathbf{y},\mathbf{z}}(\overline{(a,b)}) = T_{\mathbf{x}}^{2^{n-3}}(\overline{(a,b)})$ for every $\overline{(a,b)} \in Q_{2^n}^{\alpha}$, or equivalently

$$\overline{(-\alpha(a),b)} = \overline{((1+(-1)^{b+1})2^{n-3}+a,b)}.$$

Since we have equality in the second coordinates, this implies

$$(-2^{n-1}+1)a = (1+(-1)^{b+1})2^{n-3}+a.$$

Again, this must hold for any choice of $\overline{(a,b)}$, so let $b=0$. This implies that $-2^{n-2}+1=1$, which is a contradiction. Thus, $\gamma \neq T_{\mathbf{x}}^{2^{n-3}}$, so it must be the case that $\gamma = 1$, giving that $H \cap K = \{1\}$.

From Lemma 4.30 and Corollary 4.26, it follows that $\mathrm{Inn}(Q_{2^n}^{\alpha}) = \langle T_{\mathbf{x}}, T_{\mathbf{y}}, T_{\mathbf{y}}R_{\mathbf{y},\mathbf{z}}\rangle$, so H and K generate the entire inner mapping group.

Lastly, we show that both H and K are normal in $\mathrm{Inn}(Q_{2^n}^{\alpha})$. Since $Q_{2^n}^{\alpha}$ is an automorphic loop, it follows that for any $\gamma \in \mathrm{Inn}(Q_{2^n}^{\alpha})$, $\gamma T_u \gamma^{-1} = T_{\gamma(u)}$ and $\gamma R_{u,v}\gamma^{-1} = R_{\gamma(u),\gamma(v)}$. Since $\langle T_{\mathbf{x}}, T_{\mathbf{y}}\rangle = \mathrm{MInn}(Q_{2^n}^{\alpha})$, we have that

$$\gamma T_{\mathbf{x}}\gamma^{-1} = T_{\gamma(\mathbf{x})} \in \langle T_{\mathbf{x}}, T_{\mathbf{y}}\rangle$$

and similarly,

$$\gamma T_{\mathbf{y}}\gamma^{-1} = T_{\gamma(\mathbf{y})} \in \langle T_{\mathbf{x}}, T_{\mathbf{y}}\rangle.$$

Thus, K is normal in $\operatorname{Inn}(Q^{\alpha}_{2^n})$.

To see that H is normal we note as well that for any γ in the inner mapping group,

$$\gamma R_{\mathbf{y},\mathbf{z}}\gamma^{-1} = R_{\gamma(\mathbf{y}),\gamma(\mathbf{z})}.$$

Moreover, for $\gamma \in \operatorname{Inn}(Q^{\varphi}_{2^n})$, $\gamma\overline{(a,b)} = \overline{(a',b)}$ for some a'. That is, any inner mapping preserves the second coordinate. We claim now that the inner mappings preserve evenness in the first coordinate when the second coordinate is equal to 1. To illustrate this, we calculate on the generators:

$$\begin{aligned}
R_{\mathbf{y},\mathbf{z}}(\overline{(2k,1)}) &= \overline{(\alpha(2k),1)} = \overline{(-2k,1)}\\
T_{\mathbf{y}}(\overline{(2k,1)}) &= (-2k,1)\\
R_{\mathbf{x},\mathbf{z}}(\overline{(2k,1)}) &= \overline{((-1)^2(\alpha(1)-1)+2k,1)} = \overline{(2^{n-2}-2+2k,1)}\\
T_{\mathbf{x}}(\overline{(2k,1)}) &= \overline{((1+(-1)^2)+2k,1)} = \overline{(2+2k,1)}
\end{aligned}$$

Now, notice

$$\begin{aligned}
T_{\overline{(u,1)}}R_{\overline{(u,1)},\overline{(v,1)}}(\overline{(a,b)}) &= T_{\overline{(u,1)}}(\overline{((-1)^{b+1}\alpha(\alpha^b(u)-u)+\alpha(a),b)})\\
&= \overline{((1+(-1)^{b+1})u+(-1)[(-1)^{b+1}\alpha(\alpha^b(u)-u)+\alpha(a)],b)}\\
&= \overline{((1+(-1)^{b+1})u+(-1)^b\alpha(\alpha^b(u)-u)-\alpha(a),b)}
\end{aligned}$$

For b even, the above becomes $\overline{(-\alpha(a), b)} = T_{\mathbf{y}} R_{\mathbf{y},\mathbf{z}}(\overline{(a, b)})$. For b odd and u even, we have $\overline{(2u - \alpha(-u - u) - \alpha(a), b)} = \overline{(2u - 2u - \alpha(a), b)} = \overline{(-\alpha(a), b)} = T_{\mathbf{y}} R_{\mathbf{y},\mathbf{z}}(\overline{(a, b)})$ as well. Thus, it suffices to show that $\gamma(\mathbf{y}) = \overline{(2k, 1)}$ for some k. However, since $\mathbf{y} = \overline{(0, 1)}$ and each generator of $\operatorname{Inn}(Q^{\alpha}_{2^n})$ preserves evenness in the first coordinate when the second is equal to 1, it follows that $\gamma(\mathbf{y}) = \overline{(u, 1)}$ with u is even, so

$$\gamma T_{\mathbf{y}} R_{\mathbf{y},\mathbf{z}} \gamma^{-1} = T_{\gamma(\mathbf{y})} R_{\gamma(\mathbf{y}),\gamma(\mathbf{z})} = T_{\mathbf{y}} R_{\mathbf{y},\mathbf{z}}.$$

So H is normal as well.

Thus, $\operatorname{Inn}(Q^{\alpha}_{2^n}) = H \times K \cong \mathbb{Z}_2 \times D_{2^{n-1}}$. □

Theorem 4.32. $\operatorname{Inn}(Q^{\beta}_{2^n}) \cong \mathbb{Z}_2 \times D_{2^{n-1}}$

Proof. Let $H := \langle R_{\mathbf{y},\mathbf{z}} \rangle$ and $K := \langle T_{\mathbf{x}}, T_{\mathbf{y}} \rangle$. We claim that $\operatorname{Inn}(Q^{\beta}_{2^n}) = H \times K$. First recall that in $Q^{\beta}_{2^n}$,

$$R_{\mathbf{x},\mathbf{z}}(a, b) = ((-1)^b(\beta^b(1) - 1) + a, b).$$

For b even, $R_{\mathbf{x},\mathbf{z}}(a, b) = (a, b)$ and for b odd, $R_{\mathbf{x},\mathbf{z}}(a, b) = (2^{n-2} + a, b)$. Thus,

$$R_{\mathbf{x},\mathbf{z}}(a, b) = T_{\mathbf{x}}^{2^{n-3}}(a, b)$$

so $\operatorname{Inn}(Q^{\beta}_{2^n}) = \langle R_{\mathbf{y},\mathbf{z}}, T_{\mathbf{x}}, T_{\mathbf{y}} \rangle$.

To see that the intersection of H and K is trivial, let $\gamma \in H \cap K$ such that $\gamma \neq 1$. Since $\gamma \in H$, $|\gamma| = 2$ (again, $|R_{\mathbf{y},\mathbf{z}}| = 2$) and because it is not the identity, $\gamma = R_{\mathbf{y},\mathbf{z}}$. Since $\gamma \in K$, it can be written as $T_{\mathbf{x}}^s T_{\mathbf{y}}^r$. Using the same argument as the previous proof, since γ has order 2, γ must be either $T_{\mathbf{x}}^m T_{\mathbf{y}}$ for $0 \leq m < 2^{n-2}$ or $\gamma = T_{\mathbf{x}}^{2^{n-3}}$. In the first case, this implies, for every $\overline{(a, b)} \in Q^{\beta}_{2^n}$,

$$\overline{(\beta(a), b)} = \overline{((1 + (-1)^{b+1})m + (-1)a, b)}.$$

Taking $b = 0$, this means $(2^{n-2}+1)a = (-1)a$ or $2^{n-2}+1 = -1$, which is a contradiction, so $\gamma \neq T_{\mathbf{x}}^m T_{\mathbf{y}}$. For the second case, this would imply

$$\overline{(\beta(a), b)} = \overline{((1 + (-1)^{b+1})2^{n-3} + a, b)}.$$

Again, this must hold for any $\overline{(a, b)} \in Q_{2^n}^{\beta}$, so take $b = 0$. This gives $2^{n-2} + 1 = 1$, which is also a contradiction. Thus, $\gamma \neq T_{\mathbf{x}}^{2^{n-3}}$. Since these are the only possibilities for γ, we then conclude that for $\gamma \in H \cap K$, $\gamma = 1$. Thus, $H \cap K = \{1\}$.

For the normality of H and K, we use the same argument as the previous proof to conclude that $K \trianglelefteq \mathrm{Inn}(Q_{2^n}^{\beta})$. To see that $H \trianglelefteq \mathrm{Inn}(Q_{2^n}^{\beta})$, we again note that for $\gamma \in \mathrm{Inn}(Q_{2^n}^{\beta})$, $\gamma R_{\mathbf{y},\mathbf{z}} \gamma^{-1} = R_{\gamma(\mathbf{y}),\gamma(\mathbf{z})}$. Using Lemma 4.7, the following identities hold for any $k \in \mathbb{Z}_{2^{n-1}}$:

$$\begin{aligned}
R_{\mathbf{y},\mathbf{z}}(\overline{(2k, 1)}) &= \overline{(\beta(2k), 1)} = \overline{(2k, 1)} \\
T_{\mathbf{y}}(\overline{(2k, 1)}) &= \overline{(-2k, 1)} \\
R_{\mathbf{x},\mathbf{z}}(\overline{(2k, 1)}) &= \overline{((-1)^2(\beta(1) - 1) + 2k, 1)} = \overline{(2k, 1)} \\
T_{\mathbf{x}}(\overline{(2k, 1)}) &= \overline{(2 + 2k, 1)}
\end{aligned}$$

Thus, just as in the previous proof, $\varphi \in \mathrm{Inn}(Q_{2^n}^{\beta})$ preserves evenness in the first coordinate when the second coordinate is 1. Moreover,

$$R_{\overline{(u,1)},\overline{(v,1)}}(\overline{(a, b)}) = \overline{((-1)^{b+1}\beta(\beta^b(u) - u) + \beta(a), b)}.$$

For u even, this reduces to $\overline{(\beta(a), b)} = R_{\mathbf{y},\mathbf{z}}(\overline{(a, b)})$. Since $\mathbf{y} = \overline{(0, 1)}$ is in the form (even, 1), it then follows that $\gamma(\mathbf{y}) = \overline{(2k, 1)}$ for some k. Thus, $R_{\gamma(\mathbf{y}),\gamma(\mathbf{z})} = R_{\mathbf{y},\mathbf{z}}$, so H is normal in $\mathrm{Inn}(Q^{\beta}_{2^n})$. This shows that $\mathrm{Inn}(Q^{\beta}_{2^n}) = H \times K \cong \mathbb{Z}_2 \times D_{2^{n-1}}$. □

4.5.3 Quaternionic automorphic loops modulo their centers.

Quaternionic automorphic loops modulo their centers. Just as the structure of the inner mapping group of a loop is important, the structure of the loop modulo its center can sometimes tell us about the structure of the original loop. In this section, we explore each of the three quaternionic automorphic loops modulo their centers and prove that they are isomorphic to a generalized dihedral group (in the case of β), or a dihedral automorphic loop. The immediate consequence of these theorems is then that quaternionic automorphic loops of order 2^n are nilpotent of class $n - 1$. Moreover, these results in combination with the results from §4.5.2 allow us to finally prove that each of the automorphisms α, β, ι produce a distinct quaternionic automorphic loop.

Theorem 4.33. Given $Q = Q^{\beta}_{2^n}$, the map from Q to $\mathrm{Inn}(Q)$ sending $x \mapsto T_x$ is a homomorphism.

Proof. Let $\overline{(a, b)}, \overline{(c, d)}, \overline{(u, v)} \in Q$. Then

$$\begin{aligned}
&T_{\overline{(a,b)}\cdot\overline{(c,d)}}(\overline{(u, v)})\\
&= T_{\overline{(\beta^{bd}(a+(-1)^b c),b+d)}}(\overline{(u, v)})\\
&= \overline{((1 + (-1)^{v+1})\beta^{bd}(a + (-1)^b c) + (-1)^{b+d}u, v)}\\
&= \overline{(\beta^{bd}(a) + (-1)^b\beta^{bd}(c) + (-1)^{v+1}\beta^{bd}(a) + (-1)^{v+1+b}\beta^{bd}(c) + (-1)^{b+d}u, v)}. \qquad (**)
\end{aligned}$$

Also,

$$\begin{aligned}
&T_{\overline{(a,b)}}T_{\overline{(c,d)}}(\overline{(u, v)})\\
&= T_{\overline{(a,b)}}(\overline{((1 + (-1)^{v+1})c + (-1)^d u, v)})
\end{aligned}$$

$$\begin{aligned}&= \overline{((1+(-1)^{v+1})a+(-1)^b[(1+(-1)^{v+1})c+(-1)^d u], v)}\\ &= \overline{(a+(-1)^{v+1}a+(-1)^b c+(-1)^{b+v+1}c+(-1)^{b+d}u, v)}. \qquad (***)\end{aligned}$$

Since the second coordinates in $(**)$ and $(***)$ are equal, it follows that

$$T_{\overline{(a,b)}\cdot\overline{(c,d)}}\overline{(u,v)} = T_{\overline{(a,b)}}T_{\overline{(c,d)}}\overline{(u,v)}$$

$$\Leftrightarrow$$

$$\begin{gathered}\beta^{bd}(a)+(-1)^b\beta^{bd}(c)+(-1)^{v+1}\beta^{bd}(a)+(-1)^{v+1+b}\beta^{bd}(c)+(-1)^{b+d}u\\ = a+(-1)^{v+1}a+(-1)^b c+(-1)^{b+v+1}c+(-1)^{b+d}u.\end{gathered}$$

Canceling $(-1)^{b+d}u$ on both sides yields the equivalent condition

$$\begin{gathered}\beta^{bd}(a)+(-1)^b\beta^{bd}(c)+(-1)^{v+1}\beta^{bd}(a)+(-1)^{v+1+b}\beta^{bd}(c)\\ = a+(-1)^{v+1}a+(-1)^b c+(-1)^{b+v+1}c.\end{gathered}$$

Moving all terms with a to the left and all terms with c to the right gives equivalently:

$$T_{\overline{(a,b)}\cdot\overline{(c,d)}}\overline{(u,v)} = T_{\overline{(a,b)}}T_{\overline{(c,d)}}\overline{(u,v)}$$

$$\Leftrightarrow$$

$$\begin{gathered}\beta^{bd}(a)+(-1)a+(-1)^v a+(-1)^{v+1}\beta^{bd}(a)\\ = (-1)^{b+1}\beta^{bd}(c)+(-1)^{v+b}\beta^{bd}(c)+(-1)^b c+(-1)^{b+v+1}c.\end{gathered}$$

Suppose first that bd is even. Then β^{bd} is the identity and the equation above reduces to $0=0$, which is certainly true. So $T_{\overline{(a,b)}\cdot\overline{(c,d)}}\overline{(u,v)} = T_{\overline{(a,b)}}T_{\overline{(c,d)}}\overline{(u,v)}$ in this case.

Now suppose bd is odd and recall that $\beta = 2^{n-2} + 1$. Then the equation above becomes

$$\begin{aligned} (2^{n-2}+1)a + (-1)a + &(-1)^{v}a + (-1)^{v+1}(2^{n-2}+1)a \\ = (-1)^{b+1}(2^{n-2}+1)c + (-1)^{v+b}&(2^{n-2}+1)c + (-1)^{b}c + (-1)^{b+v+1}c, \end{aligned}$$

or, equivalently,

$$\begin{aligned} &2^{n-2}a + a + (-1)a + (-1)^{v}a + (-1)^{v+1}2^{n-2}a + (-1)^{v+1}a \\ = (-1)^{b+1}2^{n-2}c + &(-1)^{b+1}c + (-1)^{v+b}2^{n-2}c + (-1)^{v+b}c + (-1)^{b}c + (-1)^{b+v+1}c. \end{aligned}$$

This then reduces to

$$2^{n-2}a + (-1)^{v+1}2^{n-2}a = (-1)^{b+1}2^{n-2}c + (-1)^{v+b}2^{n-2}c.$$

Again, we have two cases. In the first case, if v is even, the equation above reduces to $0 = 0$, which is true. In the second case, if v is odd, the equation above becomes

$$2 \cdot 2^{n-2}a = (-1)^{b+1}2 \cdot 2^{n-2}c.$$

Since $2 \cdot 2^{n-2} = 2^{n-1} \equiv 0$ in $\mathbb{Z}_{2^{n-1}}$, this also reduces to $0 = 0$. Thus, $T_{\overline{(a,b)}\cdot\overline{(c,d)}}\overline{(u,v)} = T_{\overline{(a,b)}}T_{\overline{(c,d)}}\overline{(u,v)}$, as desired.

□

Corollary 4.34. For $Q = Q^{\beta}_{2^n}$, $Q/Z(Q) \cong \mathrm{MInn}(Q) \cong D_{2^{n-1}}$.

Proof. Using the onto homomorphism $\psi : Q \to \mathrm{MInn}(Q)$ sending $x \mapsto T_x$ from Theorem 4.33, all that is left to show is that $\ker(\psi) = Z(Q)$. We have that $\ker(\psi) = C(Q)$, and then an application of Proposition 4.22 gives the rest. □

Theorem 4.35. For $Q = Q^{\iota}_{2^n}$ and D the dihedral automorphic loop constructed with $G = \mathbb{Z}_{2^{n-2}}$, $m = 2$, and $\varphi = -1$, $Q/Z(Q) \cong D$.

Proof. Consider the map $\psi : (Q, \cdot) \to (D, *)$ given by $\psi(\overline{(a,b)}) = (a \mod 2^{n-2}, b \mod 2)$. To show this map is well-defined, suppose $\overline{(a,b)} = \overline{(c,d)}$. If $(a,b) = (c,d)$ then we are done, so suppose that $(a,b) \neq (c,d)$. Since they have the same equivalence classes, then it must be that $(c,d) = (a,b) \cdot (2^{n-2}, 2)$. However, $(a,b) \cdot (2^{n-2}, 2) = ((-1)^{2b}(a + (-1)^b 2^{n-2}), b + 2) \equiv (a,b)$ in D. Thus, $\psi(\overline{(a,b)}) = (a,b) \equiv_D (c,d) = \psi(\overline{(c,d)})$.

Now to show ψ is a homomorphism, let $\overline{(a,b)}, \overline{(c,d)} \in Q$. Then

$$\begin{aligned}
\psi(\overline{(a,b)} \cdot \overline{(c,d)}) &= \psi(\overline{((-1)^{bd}(a + (-1)^b c), b + d)}) \\
&= ((-1)^{bd}(a + (-1)^b c) \mod 2^{n-2}, b + d \mod 2) \\
&= (a,b) * (c,d) \\
&= \psi(\overline{(a,b)}) * \psi(\overline{(c,d)}).
\end{aligned}$$

Lastly, we notice that the kernel of ψ is:

$$\begin{aligned}
\ker \psi &= \{\overline{(u,v)} \in Q : \psi(\overline{(u,v)}) = (0,0)\} \\
&= \{\overline{(u,v)} \in Q : (u,v) \equiv_D (0,0)\} \\
&= \{(0,0), (0,2), (2^{n-2}, 0), (2^{n-2}, 2)\} \\
&= Z(Q).
\end{aligned}$$

Thus, $Q/Z(Q) \cong D$, as desired. □

Theorem 4.36. For $Q = Q^{\alpha}_{2^n}$ and D the dihedral automorphic loop constructed with $G = \mathbb{Z}_{2^{n-2}}$, $m = 2$, and $\varphi = -1$, $Q/Z(Q) \cong D$.

Proof. Same proof as above, but we notice instead:

$$\psi(\overline{(a,b)(c,d)}) = \psi(\overline{((2^{n-2}-1)^{bd}(a+(-1)^b c), b+d)}) = ((2^{n-2}-1)^{bd}(a+(-1)^b c), b+d).$$

Now, since $|\,\alpha\,| = 2$, either $((2^{n-2}-1)^{bd}(a+(-1)^b c), b+d) = (a+(-1)^b c, b+d)$ if bd is even, or $((2^{n-2}-1)^{bd}(a+(-1)^b c), b+d) = ((2^{n-2}-1)(a+(-1)^b c), b+d)$ if bd is odd. In the former case, we see that $((2^{n-2}-1)^{bd}(a+(-1)^b c), b+d) = (a+(-1)^b c, b+d) = ((-1)^{bd}(a+(-1)^b c), b+d) = (a,b)(c,d) = \psi(\overline{(a,b)})\psi(\overline{(c,d)})$. In the latter case, we have $((2^{n-2}-1)^{bd}(a+(-1)^b c), b+d) = ((2^{n-2}-1)(a+(-1)^b c), b+d) = ((-1)(a+(-1)^b c), b+d) = ((-1)^{bd}(a+(-1)^b c), b+d) = (a,b)(b,d) = \psi(\overline{(a,b)})\psi(\overline{(c,d)})$. Thus, ψ is a homomorphism here as well, and the isomorphism follows as above. □

Corollary 4.37. $Q_{2^n}^{\alpha}/Z(Q_{2^n}^{\alpha}) \cong Q_{2^n}^{\iota}/Z(Q_{2^n}^{\iota})$.

With the description of the inner mapping groups given in the previous subsection and the structure of the quotient loops proved in this subsection, we are now able to show that each distinct automorphism produces a distinct quaternionic automorphic loop. We state this more precisely in the following theorem.

Theorem 4.38. Each distinct $\varphi \in \mathrm{Aut}(\mathbb{Z}_{2^{n-1}})$ with $|\varphi| = 2$ produces a distinct (up to isomorphism) quaternionic automorphic loop of order 2^n.

Proof. While there are several differences between the loops to point to, we limit our attention to their inner mapping groups and the quotient of the loops by their centers. First, $Q_{2^n}^{\alpha} \ncong Q_{2^n}^{\beta}$ since $Q_{2^n}^{\alpha}/Z(Q_{2^n}^{\alpha}) \ncong Q_{2^n}^{\beta}/Z(Q_{2^n}^{\beta})$ and $Q_{2^n}^{\iota} \ncong Q_{2^n}^{\beta}$ since $Q_{2^n}^{\iota}/Z(Q_{2^n}^{\iota}) \ncong Q_{2^n}^{\beta}/Z(Q_{2^n}^{\beta})$ by Theorems 4.36 and 4.35 and Corollary 4.34. Moreover, $Q_{2^n}^{\alpha} \ncong Q_{2^n}^{\iota}$ since $\mathrm{Inn}(Q_{2^n}^{\alpha}) \ncong \mathrm{Inn}(Q_{2^n}^{\iota})$ by Theorems 4.31 and 4.29. □

4.5.4 Nilpotency.

Theorem 4.39. For $Q = Q_{2^n}^{\varphi}$, Q is nilpotent of class $n-1$.

Proof. By Corollary 4.34, $Q_{2^n}^{\beta}/Z(Q_{2^n}^{\beta}) \cong D_{2^{n-1}}$. It is well known [12] that the dihedral group of order 2^{n-1} is nilpotent of class $n-2$, thus $Q_{2^n}^{\beta}$ is nilpotent of class $n-1$. Moreover, we have by Theorems 4.36 and 4.35 that $Q_{2^n}^{\alpha}/Z(Q_{2^n}^{\alpha}) \cong Q_{2^n}^{\iota}/Z(Q_{2^n}^{\iota}) \cong D$ where D is the dihedral-like automorphic loop constructed with $G = \mathbb{Z}_{2^{n-2}}$, $m = 2$, and $\varphi = -1$. Aboras shows in [1] that D has nilpotency class $n-2$. Again, this implies $Q_{2^n}^{\iota}$ and $Q_{2^n}^{\alpha}$ have nilpotency class $n-1$.

□

4.5.5 Subloop structure of $Q_{2^n}^{\beta}$.

Before understanding the subloop structure, we make a note here that, while loops (even automorphic loops) do not in general satisfy the Lagrange Property, it follows from the fact that automorphic 2-loops are solvable [17] that quaternionic automorphic loops in particular do have the Lagrange Property [10]. Thus, in the discussion which follows, we may make the usual order considerations.

Lemma 4.40. In $Q_{2^n}^{\beta}$, the subloops $\langle \mathbf{x}^2, \mathbf{y} \rangle$ and $\langle \mathbf{x}^2, \mathbf{xy} \rangle$ are associative, of order 2^{n-1}, and normal in $Q_{2^n}^{\beta}$.

Proof. Recall that the condition on associativity given by (4.20) is

$$\overline{(a,l)} \cdot \overline{(b,m)(c,k)} = \overline{(a,l)(b,m)} \cdot \overline{(c,k)}$$

$$\Leftrightarrow$$

$$\varphi^{lm}(a) + (-1)^{m+l}\varphi^{lm+mk}(c) = \varphi^{mk+lm}(a) + (-1)^{m+l}\varphi^{mk}(c).$$

Let $\overline{(a,l)}, \overline{(b,m)}, \overline{(c,k)} \in \langle \mathbf{x}^2, \mathbf{y} \rangle$. By Lemma 4.7 we have that a, b, and c are even and so $\beta(a) = a$ and $\beta(c) = c$. Thus, the associativity condition reduces to the identity $a + (-1)^{m+l}c = a + (-1)^{m+l}c$, so $\langle \mathbf{x}^2, \mathbf{y} \rangle$ is associative.

Now suppose $\overline{(a,l)}, \overline{(b,m)}, \overline{(c,k)} \in \langle \mathbf{x}^2, \mathbf{xy}\rangle$. Lemma 4.7 gives that for any $\overline{(a,l)} \in \langle \mathbf{x}^2, \mathbf{xy}\rangle$, either a is even and $l = 0$, i.e. $\overline{(a,l)} \in \langle \mathbf{x}^2\rangle$, or a is odd and $l = 1$. If $\overline{(a,l)}, \overline{(b,m)}, \overline{(c,k)} \in \langle \mathbf{x}^2\rangle$, then $(a,l), (b,m)$, and (c,k) associate since automorphic loops are power associative. Moreover, if $\overline{(b,m)} \in \langle \mathbf{x}^2\rangle$, we have from Proposition 4.16 that

$$\overline{(a,l)} \cdot \overline{(b,m)(c,k)} = \overline{(a,l)(b,m)} \cdot \overline{(c,k)}.$$

So suppose that $\overline{(b,m)} \notin \langle \mathbf{x}^2\rangle$. Then by the discussion above, b is odd and $m = 1$. In this case, (4.20) holds if and only if

$$\beta^l(a) + (-1)^{l+1}\beta^{l+k}(c) = \beta^{k+l}(a) + (-1)^{1+l}\beta^k(c).$$

We now have three cases: a is even and c is odd, a is odd and c is even, or both a and c are odd.

For the first case, if a is even and c is odd, then $l = 0$ and $k = 1$. So (4.20) holds if and only if

$$a + (-1)\beta(c) = \beta(a) + (-1)\beta(c).$$

Since a is even, Lemma 4.7 gives $\beta(a) = a$, so (4.20) holds in this case.

For the second case, if a is odd and c is even, then $l = 1$ and $k = 0$, so the associativity condition gives

$$\beta(a) + \beta(c) = \beta(a) + c.$$

Again, since c is even, $\beta(c) = c$, so this is an identity as well.

For the third case, if a and c are odd, then $l = k = 1$, so (4.20) holds if and only if

$$\beta(a) + c = a + \beta(c).$$

From the proof of Lemma 4.7, we see that $\beta(a) = a + 2^{n-2}$ when a is odd, so the above holds if and only if

$$a + 2^{n-2} + c = a + c + 2^{n-2},$$

which holds as well. These are all the cases, so we have for every $\overline{(a,l)}, \overline{(b,m)}, \overline{(c,k)} \in \langle \mathbf{x}^2, \mathbf{xy} \rangle$, $\overline{(a,l)} \cdot \overline{(b,m)(c,k)} = \overline{(a,l)(b,m)} \cdot \overline{(c,k)}$, as desired.

Now, since $|\mathbf{x}^2| = 2^{n-2}$ and $\langle \mathbf{x}^2 \rangle < \langle \mathbf{x}^2, \mathbf{y} \rangle, \langle \mathbf{x}^2, \mathbf{xy} \rangle < Q^{\beta}_{2^n}$, we have that $|\langle \mathbf{x}^2, \mathbf{y} \rangle| = 2^{n-1}$ and $|\langle \mathbf{x}^2, \mathbf{xy} \rangle| = 2^{n-1}$.

Since each subgroup has index 2 in $Q^{\beta}_{2^n}$, it follows that they are both normal in $Q^{\beta}_{2^n}$.

□

Lemma 4.41. For any noncyclic $N \trianglelefteq Q^{\beta}_{2^n}$, $\mathbf{x}^2 \in N$.

Proof. Let $N \trianglelefteq Q^{\beta}_{2^n}$ such that N is not cyclic. In particular, $N \not\subseteq \langle \mathbf{x} \rangle$, so there is some $g \in N$ so that $g = \mathbf{x}^a\mathbf{y} = \overline{(a,1)}$. Since N is normal, it is fixed by all the inner mappings. Thus, $g \cdot T_{\mathbf{x}}(g^{-1}) \in N$. We note here that $g^{-1} \in Q^{\beta}_{2^n} = \overline{(c,d)}$ such that $\overline{(a,1)} \cdot \overline{(c,d)} = \overline{(0,0)}$, or $\overline{(\beta^d(a + (-1)c), 1 + d)} = \overline{(0,0)}$. Solving for c and d, we get that $g^{-1} = \overline{(a,-1)}$. So, calculating:

$$\begin{aligned} g \cdot T_{\mathbf{x}}(g^{-1}) &= \overline{(a,1)} \cdot T_{\mathbf{x}}\overline{(a,-1)} \\ &= \overline{(a,1)} \cdot \overline{((1 + (-1)^0) + a, -1)} \\ &= \overline{(a,1)} \cdot \overline{(2 + a, -1)} \\ &= \overline{(\beta^{-1}(a + (-1)(2 + a)), 0)} \\ &= \overline{(\beta(-2), 0)} \\ &= \overline{(-2, 0)} \\ &= \mathbf{x}^{-2}. \end{aligned}$$

Since $\mathbf{x}^{-2} \in N$, so is $\mathbf{x}^2$. Thus, if N is normal in $Q^{\beta}_{2^n}$ and noncyclic, $\mathbf{x}^2 \in N$. □

Corollary 4.42. The only proper, noncyclic, normal subloops of $Q_{2^n}^{\beta}$ are $\langle \mathbf{x}^2, \mathbf{y} \rangle$ and $\langle \mathbf{x}^2, \mathbf{xy} \rangle$.

Proof. Let N be a proper, noncylic, normal subloop of $Q_{2^n}^{\beta}$. By Lemma 4.41, $\langle \mathbf{x}^2 \rangle \leq N$. Let $k \in \mathbb{Z}_{2^{n-1}}$. Since $\mathbf{x} \in N_{\mu}$, $R_{\mathbf{x},\mathbf{z}}(\overline{(2k,0)}) = R_{\mathbf{y},\mathbf{z}}(\overline{(2k,0)}) = \overline{(2k,0)}$. Moreover, since $Q_{2^n}^{\beta}$ is power associative, $T_{\mathbf{x}}(\overline{(2k,0)}) = \overline{(2k,0)}$. Lastly, we note $T_{\mathbf{y}}(\overline{(2k,0)}) = \overline{(-2k,0)}$, so all inner mappings preserve evenness in the first coordinate when the second coordinate is 0. Thus, $\langle \mathbf{x}^2 \rangle$ is normal in $Q_{2^n}^{\beta}$, with index $[Q_{2^n}^{\beta} : \langle \mathbf{x}^2 \rangle] = \frac{2^n}{2^{n-2}} = 4$. So $\langle \mathbf{x}^2 \rangle$ splits $Q_{2^n}^{\beta}$ into 4 cosets, we claim with representatives $\{\overline{(0,0)}, \mathbf{x}, \mathbf{y}, \mathbf{xy}\}$. To see this, let $g \in Q_{2^n}^{\beta}$. Then $g = \mathbf{x}^a$ or $g = \mathbf{x}^a\mathbf{y}$ for some a, by Lemma 4.13. If $g = \mathbf{x}^a$ with a odd, then $g \in \langle \mathbf{x}^2 \rangle \mathbf{x}$. If $g = \mathbf{x}^a$ with a even, then $g \in \langle \mathbf{x}^2 \rangle$. In the case where $g = \mathbf{x}^a\mathbf{y}$, if a is odd then $g \in \langle \mathbf{x}^2 \rangle \mathbf{xy}$, and if a is even, then $g \in \langle \mathbf{x}^2 \rangle \mathbf{y}$.

Since $N \neq \langle \mathbf{x}^2 \rangle$, it follows that $\langle \mathbf{x}^2 \rangle < N < Q_{2^n}^{\beta}$, so $|\langle \mathbf{x}^2 \rangle| = 2^{n-2} < |N| < 2^n = Q_{2^n}^{\beta}$. We may conclude that $|N| = 2^{n-1}$ and $[N : \langle \mathbf{x}^2 \rangle] = 2$. Thus, N is $\langle \mathbf{x}, \mathbf{x}^2 \rangle$, $\langle \mathbf{x}^2, \mathbf{y} \rangle$, or $\langle \mathbf{x}^2, \mathbf{xy} \rangle$. However, $\langle \mathbf{x}, \mathbf{x}^2 \rangle = \langle \mathbf{x} \rangle$ is cyclic, leaving us with only $N = \langle \mathbf{x}^2, \mathbf{y} \rangle$ or $N = \langle \mathbf{x}^2, \mathbf{xy} \rangle$. □

It is a fact from group theory that if Q is a 2-group, then it has a unique element of order 2 if and only if it is cyclic or generalized quaternion. For a proof, see [35]. Thus, we have the following corollary.

Corollary 4.43. For $Q_{2^n}^{\beta}$, the subloops $\langle \mathbf{x}^2, \mathbf{y} \rangle$ and $\langle \mathbf{x}^2, \mathbf{xy} \rangle$ are isomorphic to the generalized quaternion group of order 2^{n-1}.

Proof. We note that since $\mathbf{x}^{2^{n-2}} \in \langle \mathbf{x}^2 \rangle$, which is the unique element of order 2 in $Q_{2^n}^{\beta}$, and since $\langle \mathbf{x}^2, \mathbf{y} \rangle$ and $\langle \mathbf{x}^2, \mathbf{xy} \rangle$ are noncyclic and associative, then the comment above immediately gives that they are both isomorphic to a generalized quaternion group. Lemma 4.40 gives that their order is 2^{n-1}, and the result follows. □

Lemma 4.44. Let Q be a quaternionic automorphic loop of order 2^n and let $H < Q$. Then there exists a subnormal chain of subloops

$$H = H_0 \lhd H_1 \lhd \cdots \lhd H_r = Q$$

such that $|H_{i+1}/H_i| = 2$.

Proof. We proceed by induction on n. For $n = 1$, $|Q| = 2$, so H is trivial. Take $H_0 = H$ and $H_r = Q$ to satisfy the statement. Suppose the statement holds for all orders 2^m with $m < n$ and let $|Q| = 2^n$ with $H < Q$. Since $Z(Q)$ is contained in every subloop of Q by Corollary 4.15 and $Z(Q) \neq 1$ by Proposition 4.22, $H/Z(Q)$ and $Q/Z(Q)$ have order strictly less than H and Q, respectively. By the induction hypothesis, there is a subnormal chain

$$H/Z(Q) = H_0 \lhd H_1 \lhd \cdots \lhd H_r = Q/Z(Q)$$

such that $|H_{i+1}/H_i| = 2$ for every $i < r$. The isomorphism theorems for loops then give some $\overline{H_i} < Q$ such that $\overline{H_i}/Z(Q) = H_i$, $\overline{H_i} \lhd \overline{H_{i+1}}$, and $[\overline{H_{i+1}} : \overline{H_i}] = [H_{i+1} : H_i] = 2$, which yields the desired chain. □

In particular, Lemma 4.44 says that given any $H < Q$, $H \leq H_{r-1}$ such that $[Q : H_{r-1}] = 2$. We formalize this in the following corollary.

Corollary 4.45. Every proper subloop of a quaternionic automorphic loop is contained in a subloop of index 2.

Now, since every proper subloop is contained in a subloop of index 2, and since any subloop of index 2 must be normal, and since the only noncyclic proper normal subloops of $Q_{2^n}^{\beta}$ are $\langle \mathbf{x}^2, \mathbf{y} \rangle$ and $\langle \mathbf{x}^2, \mathbf{xy} \rangle$, it follows immediately that:

Corollary 4.46. Every proper noncyclic subloop of $Q_{2^n}^{\beta}$ is contained in $\langle \mathbf{x}^2, \mathbf{y} \rangle$ or $\langle \mathbf{x}^2, \mathbf{xy} \rangle$.

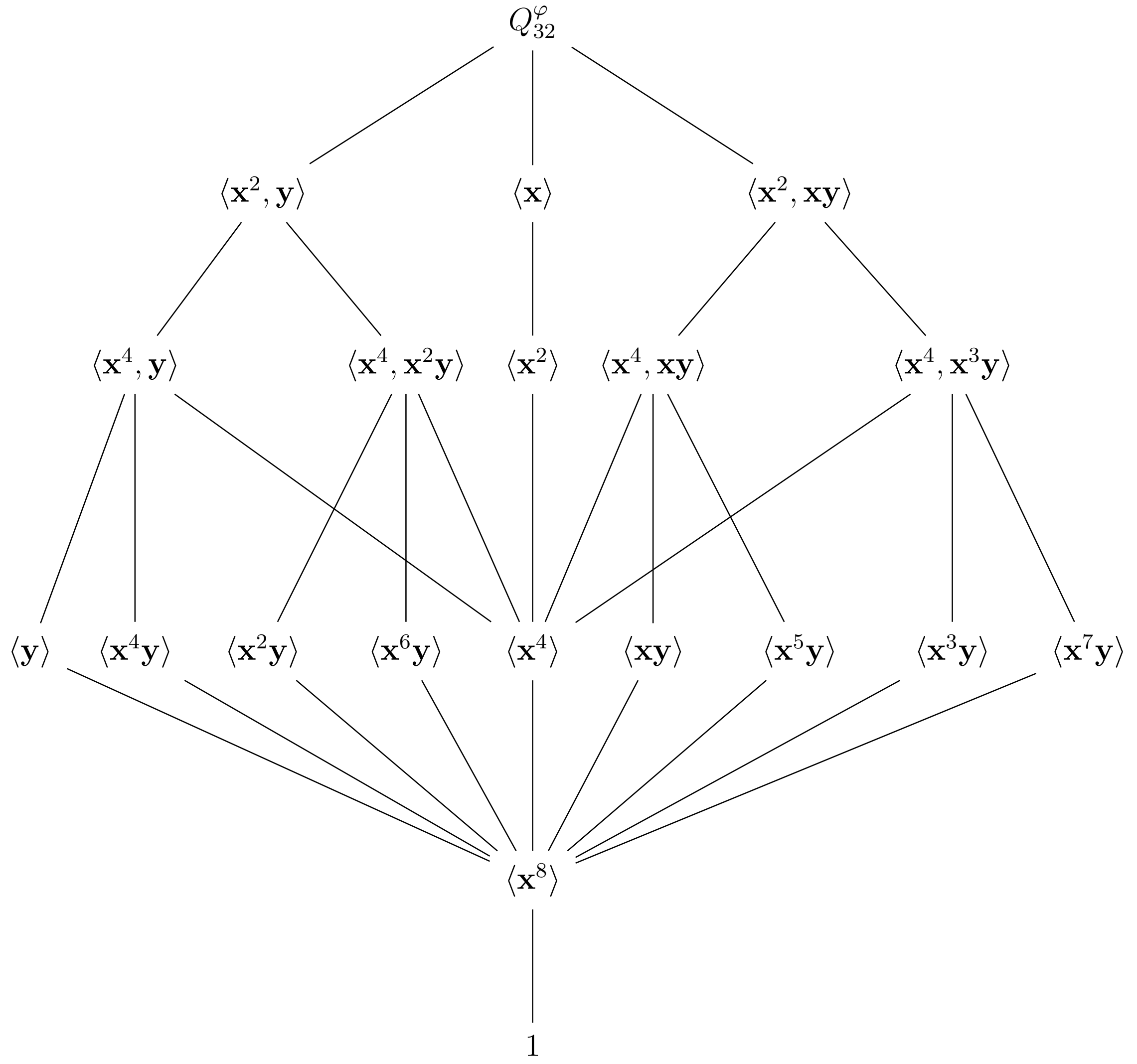
Theorem 4.47. All proper subloops of $Q^{\beta}_{2^n}$ are either cyclic groups or generalized quaternion groups.

Proof. Let $H < Q^{\beta}_{2^n}$. If H is cyclic then it is associative since automorphic loops are power associative. So H is a cyclic group in this case. Suppose that H is not cyclic. Corollary 4.46 gives that $H \leq \langle \mathbf{x}^2, \mathbf{y} \rangle$ or $H \leq \langle \mathbf{x}^2, \mathbf{xy} \rangle$. However, Corollary 4.43 gives that $\langle \mathbf{x}^2, \mathbf{y} \rangle$ and $\langle \mathbf{x}^2, \mathbf{xy} \rangle$ are isomorphic to the generalized quaternion group of order 2^{n-1}. Since every subgroup of a generalized quaternion group is either a cyclic group or a generalized quaternion group, the result follows immediately. □

Since $\alpha(2k) = \iota(2k) = -2k$ for any integer k, we can easily modify the proof of Lemma 4.41 to show that $\mathbf{x}^2 \in N$ for any normal, noncyclic subloop N of any quaternionic automorphic loop. Since Lemma 4.44 is also done in general for any quaternionic automorphic loop, we have that every subloop of any quaternionic automorphic loop is contained in an index 2 subloop. These facts combined with some GAP calculations, give us that the subloop lattice of all three quaternionic automorphic loops of order 32 are isomorphic. That is, the following lattice applies to any Q^{φ}_{32}.

Moreover, one may note that in the lattice of congruences of Q^{φ}_{32}, $\langle \mathbf{x}^8 \rangle = Z(Q^{\varphi}_{32})$ is the unique smallest nontrivial congruence, which in universal algebra is termed the *monolith*. This implies that Q^{φ}_{32} is subdirectly irreducible, a fact which extends to any order 2^n.

Subloop Lattice of Q_{32}^{φ}



Q_{32}^{φ}
$\langle \mathbf{x}^2, \mathbf{y} \rangle$
$\langle \mathbf{x} \rangle$
$\langle \mathbf{x}^2, \mathbf{xy} \rangle$
$\langle \mathbf{x}^4, \mathbf{y} \rangle$
$\langle \mathbf{x}^4, \mathbf{x}^2\mathbf{y} \rangle$
$\langle \mathbf{x}^2 \rangle$
$\langle \mathbf{x}^4, \mathbf{xy} \rangle$
$\langle \mathbf{x}^4, \mathbf{x}^3\mathbf{y} \rangle$
$\langle \mathbf{y} \rangle$
$\langle \mathbf{x}^4\mathbf{y} \rangle$
$\langle \mathbf{x}^2\mathbf{y} \rangle$
$\langle \mathbf{x}^6\mathbf{y} \rangle$
$\langle \mathbf{x}^4 \rangle$
$\langle \mathbf{xy} \rangle$
$\langle \mathbf{x}^5\mathbf{y} \rangle$
$\langle \mathbf{x}^3\mathbf{y} \rangle$
$\langle \mathbf{x}^7\mathbf{y} \rangle$
$\langle \mathbf{x}^8 \rangle$
1

4.6 Further Study

With the dihedral groups and the generalized quaternion groups generalized to the automorphic loop case, the natural question now arises as to whether a similar construction can produce the automorphic loop generalization of the dicyclic groups.

Chapter 5: Quasigroups isotopic to commutative Moufang loops

5.1 Introduction

The contents of this chapter are from work done in collaboration with Michael Kinyon and make use of [29].

Throughout the course of this dissertation, we have been studying loops, whose identity element give them slightly more structure than quasigroups. In general, quasigroups can be difficult to work with and thus, one of the important ways in which quasigroups are studied is through their loop isotopes. For some interesting varieties of quasigroups, their loop isotopes live in some highly structured class of loops in such a way that the quasigroups themselves can be represented in terms of those loops. For instance, sometimes the quasigroups isotopic to some particular class of loops can be characterized in terms of nice identities. An example of this is the following characterization of quasigroups isotopic to abelian groups often attributed to Belousov [4] (see also [11]), who proved the equivalence of parts (1) and (2). The equivalence of (1) and (3) follows by symmetry.

Proposition 5.1. Let $(Q, \cdot)$ be a quasigroup. The following are equivalent.

1. $(Q, \cdot)$ is isotopic to an abelian group;
2. For all $x, y, z, u \in Q$, the identity $x(y\backslash(zu)) = z(y\backslash(xu))$ holds;
3. For all $x, y, z, u \in Q$, the identity $((xy)/z)u = ((xu)/z)y$ holds.

Throughout this chapter we will be looking at loops isotopic to quasigroups, so we will often have both a loop and a quasigroup structure on the same underlying set. Thus, we will distinguish between the operations by using multiplicative notation such as $\cdot$, $*$, or juxtaposition for quasigroups, and additive notation $+$ with neutral element 0 for loops, even if they are not necessarily commutative. We will denote the left and right translations by x in a loop $(Q, +)$ by L_x^+ and R_x^+, respectively.

As mentioned, we are looking for quasigroups which are isotopic to highly structured classes of loops. One could make the argument that without the full power of associativity, commutative Moufang loops, or CMLs, are the most structured variety of loops. However, there are several varieties which are similar to CMLs which we will explore in this chapter. We define them here as follows.

Definition 5.1. A loop $(Q, +)$ is a *left Bol loop* if it satisfies the identity $(x+(y+x))+z = x + (y + (x + z))$ for all $x, y, z \in Q$. *Right Bol loops* are defined dually, and a loop which is both left Bol and right Bol is said to be a *Moufang loop*.

It is perhaps necessary to note that this is just one of the many equivalent definitions of a Moufang loop, but it is the one which will serve our purposes best here.

Our primary interest in this chapter is in quasigroups isotopic to commutative Moufang loops. We will first find it useful to characterize quasigroups isotopic to left Bol loops and to Moufang loops. Left Bol loops form an isotopically invariant variety, that is, any loop isotopic to a left Bol loop is a left Bol loop. The same isotopism invariance holds for Moufang loops. For such varieties, it is straightforward to write down a characterization using the method first discussed by Falconer [13]. However, in Theorems 5.7 and 5.10 in §5.2, we will find more conceptual characterizations which are better suited to our purposes and which we have not been able to find in the literature.

Abelian groups also form an isotopically invariant variety, so in Proposition 5.1, it was not necessary to specify which loop isotope is an abelian group because in fact, they all are. Commutative Moufang loops, however, require more care because they do not form an isotopically invariant variety. In fact, if every loop isotopic to a given loop is a commutative Moufang loop, then the loop itself is an abelian group [33, III.6.4 and IV.5.6]. Thus, we will look specifically at a particular form of loop isotope. That is, for a quasigroup $(Q,\cdot)$ and some $u \in Q$, let the principal loop isotope $(Q,+_u)$ be of the form

$$x +_u y = (x/u)(u\backslash y)\,. \tag{5.1}$$

For the motivating varieties of quasigroups $(Q,\cdot)$ discussed below, it turns out that every principal loop isotope of this form is a commutative Moufang loop, which we will prove in §5.3. In general, the class of quasigroups $(Q,\cdot)$ such that each $(Q,+_u)$ is a commutative Moufang loop has a characterization which nicely generalizes Proposition 5.1.

Theorem 5.2. Let $(Q,\cdot)$ be a quasigroup. The following are equivalent:

1. Each loop isotope $(Q,+_u)$ is a commutative Moufang loop.
2. For all $x,y,z \in Q$, the following identity holds:

$$x(y\backslash(zz)) = z(y\backslash(xz))\,. \tag{Q1}$$

3. For all $x,y,z \in Q$, the following identity holds:

$$((zz)/y)x = ((zx)/y)z\,. \tag{Q2}$$

Isotopy only guarantees that the mappings (α,β,γ) are bijections on Q. Thus, the notion of "affine" gives a stronger relationship between quasigroups and loops.

Definition 5.2. A quasigroup $(Q,\cdot)$ is said to be *affine* over a commutative Moufang loop $(Q,+)$ if there exist $c \in Q$ and $\varphi,\psi \in \mathrm{Aut}(Q)$ such that $xy = (\varphi(x)+\psi(y))+c$ for all $x,y \in Q$. If $c = 0$, then $(Q,\cdot)$ is said to be *linear* over $(Q,+)$. The quintuple $(Q,+,\varphi,\psi,c)$ is said to be an *affine form* of $(Q,\cdot)$.

We should mention that in the literature, the definition of "affine" varies a bit from author to author; some allow more general classes of loops $(Q, +)$, some restrict $c \in Q$ to lie in the center of the loop $(Q, +)$, *etc.* In addition, the quintuples we are calling affine forms are also called "arithmetic forms".

Quasigroups which are affine over abelian groups are known as *central* quasigroups (formerly "T-quasigroups"). (This is not the definition of central quasigroup [38] but it will suffice for our purposes.) Central quasigroups form a variety and can be equationally axiomatized in various ways. For instance, one can combine Proposition 5.1(2) or (3) with a couple of other short identities [11].

In §5.4 we consider a new variety of quasigroups which we call "semiparamedial" quasigroups. Along with semimedial quasigroups (both defined below), semiparamedial quasigroups are affine over commutative Moufang loops. But first a few historical remarks are in order.

The two most well-studied varieties of central quasigroups are *medial* quasigroups (also known as *entropic*, formerly "abelian") which are defined by the identity $xy \cdot uv = xu \cdot yv$, and *paramedial* quasigroups, which are defined by the identity $xy \cdot uv = vy \cdot ux$. Part (1) of the following is the *Toyoda-Bruck-Murdoch Theorem*, the earliest example of an affine representation theorem for a variety of quasigroups.

Proposition 5.3. Let $(Q, \cdot)$ be a quasigroup.

1. $(Q, \cdot)$ is medial if and only if it has an affine form $(Q, +, \varphi, \psi, c)$ where $(Q, +)$ is an abelian group and $\varphi\psi = \psi\varphi$ [42, 5, 31].

2. $(Q, \cdot)$ is paramedial if and only if it has an affine form $(Q, +, \varphi, \psi, c)$ where $(Q, +)$ is an abelian group and $\varphi^2 = \psi^2$ [27].

Thus in some sense, the study of medial or paramedial quasigroups "reduces" to the study of abelian groups and their automorphisms.

Proposition 5.3(1) has been generalized in various ways, notably to trimedial (or terentropic, formerly tri-abelian) quasigroups [23], which also includes the case of distributive quasigroups [3, 39]. The affine representation of trimedial quasigroups turns out to be crucial to their enumeration [20]. The trimedial case was, in turn, generalized to F-quasigroups [24, 26] and semimedial quasigroups (formerly "weakly abelian" or just "WA") [25], and it is to this latter generalization we now turn. We also introduce (for what we believe to be the first time) the "para-analog" of semimedial quasigroups.

Definition 5.3. A quasigroup $(Q, \cdot)$ is *semimedial* if the following identities hold for all $x, y, z \in Q$:

$$xx \cdot yz = xy \cdot xz\,, \tag{S1}$$

$$xy \cdot zz = xz \cdot yz\,. \tag{S2}$$

A quasigroup $(Q, \cdot)$ is *semiparamedial* if the following identities hold for all $x, y, z \in Q$:

$$xx \cdot yz = zx \cdot yx\,, \tag{P1}$$

$$xy \cdot zz = zy \cdot zx\,. \tag{P2}$$

In 1978, Kepka proved the following affine representation theorem for semimedial quasigroups [25], which we present here as motivation for what follows.

Theorem 5.4. $(Q, \cdot)$ is semimedial if and only if it has an affine form $(Q, +, \varphi, \psi, c)$ where $(Q, +)$ is an abelian group and $\varphi\psi = \psi\varphi$.

Motivated by this theorem, we prove in §5.4 that a quasigroup is semiparamedial if and only if it has a specific affine form where $\varphi^2 = \psi^2$. More specifically, we prove the following theorem.

Theorem 5.5. Let $(Q,\cdot)$ be a quasigroup. Then $(Q,\cdot)$ is semiparamedial if and only if $(Q,\cdot)$ has affine form $(Q,+,\psi,\varphi,g)$ where $(Q,+)$ is a commutative Moufang loop, $\varphi^2 = \psi^2$, and $\psi\varphi^{-1}$ is a nuclear automorphism of $(Q,+)$.

5.2 Quasigroups isotopic to Bol and Moufang loops

In this section we will find a useful characterization of quasigroups isotopic to left Bol loops and thus of quasigroups isotopic to Moufang loops. Since left Bol loops form an isotopically invariant variety, there is a standard method of writing an identity which characterizes a quasigroup Q isotopic to a left Bol loop: fix $e \in Q$, consider the principal loop isotope $(Q,+_e)$, write the left Bol identity in terms of the quasigroup operations. That is, for $x,y,z \in Q$,

$$(((x/e)(e\backslash((y/e)(e\backslash x))))/e)(e\backslash z) = (x/e)(e\backslash((y/e)(e\backslash((x/e)(e\backslash z))))) .$$

Then treat e as being universally quantified so that we have an identity in 4 variables. This idea goes back to Falconer [13]. This identity can certainly be simplified (and can also be used to prove the results below), but even in a simplified form, it does not seem to be particularly elegant. The main result of this section, Theorem 5.7, seems to be both more elegant and more useful.

A quasigroup Q is said to have the *left inverse property* (LIP) if for each $x \in Q$, there exists $x^\lambda \in Q$ such that $x^\lambda \cdot xy = y$ for all $y \in Q$. Taking, say, $y = x\backslash x$, we see that $x^\lambda = (x\backslash x)/x$, and so LIP quasigroups form a variety. The *right inverse property* (RIP) is defined dually in the obvious way, and a quasigroup with both the LIP and the RIP is said to have the *inverse property* (IP).

In an additively written loop $(Q,+)$, the LIP can be written as $(-)_\lambda x + (x+y) = y$ where $(-)_\lambda x$ denotes the left inverse of x, that is, $(-)_\lambda x + x = 0$. (In fact, in LIP loops,

$(-)_\lambda x$ turns out to be a two-sided inverse for x.) The LIP can be usefully expressed in terms of left translations by $(L_x^+)^{-1} = L_{(-)_\lambda x}^+$ for all $x \in Q$.

As discussed in §5.1, for a quasigroup $(Q, \cdot)$, we are particularly interested in the loop isotopes $(Q, +_u)$ where for each $x, y, u \in Q$, $x +_u y = (x/u)(u\backslash y)$. Here the identity element is $0 = uu$ and for $x \in Q$, the left inverse of x is $-x = (0/(u\backslash x))u$. Left and right translations in $(Q, +_u)$ are, respectively, $L_x^+ = L_{x/u}L_u^{-1}$ and $R_x^+ = R_{u\backslash x}R_u^{-1}$, $x \in Q$.

Lemma 5.6. Let $(Q, \cdot)$ be a quasigroup and fix $e \in Q$. The following are equivalent.

1. $(Q, +_e)$ is an LIP loop;

2. For all $x \in Q$, $L_e L_x^{-1} L_e$ is a left translation;

3. For all $x, y, z \in Q$, $(e(x\backslash(ey)))/y = (e(x\backslash(ez)))/z$;

4. For all $x, y \in Q$, $e(x\backslash(ey)) = ((e(x\backslash e))/(e\backslash e))y$.

Proof. (1) $\implies$ (2): We have $(L_x^+)^{-1} = L_e L_{x/e}^{-1}$ and $L_{-x}^+ = L_{0/(x\backslash e)}L_e^{-1}$. Thus if $(Q, +_e)$ has the LIP, then $L_e L_{x/e}^{-1} = L_{0/(x\backslash e)}L_e^{-1}$. Multiplying on the right by L_e we get $L_e L_{x/e}^{-1} L_e = L_{0/(x\backslash e)}$. Replacing x with xe, we obtain $L_e L_x^{-1} L_e = L_{0/((xe)\backslash e)}$. Thus for each $x \in Q$, $L_e L_x^{-1} L_e$ is a left translation, and so (2) holds.

(2) $\implies$ (1): Since $L_e L_{x/e}^{-1} L_e$ is a left translation, say, L_w for some $w \in Q$, we therefore have $L_e^{-1} L_{x/e} L_e^{-1} = L_w^{-1}$. Apply both sides to $0 = ee$. The left side is $e\backslash((x/e)(e\backslash(ee))) = e\backslash x$. The right side is $w\backslash 0$. Thus $w\backslash 0 = e\backslash x$ and solving this for w yields $w = 0/(e\backslash x)$. Now we compute

$$L_{(-)_\lambda x}^+ L_x^+ = L_{0/(x\backslash e)} L_e^{-1} L_{x/e} L_e^{-1} = L_{0/(x\backslash e)} L_{0/(x\backslash e)}^{-1} = \mathrm{id}\,,$$

that is, $(Q, +_e)$ has the LIP. This proves (1).

(2) $\implies$ (3): We have $L_e L_{x/e}^{-1} L_e = L_w$ for some $w \in Q$ depending only on e and x. Thus for all y, $e(x\backslash(ey)) = wy$. Therefore $(e(x\backslash(ey)))/y$ is independent of y, which proves (3).

(3) $\implies$ (4): This follows by taking $z = e\backslash e$ and then multiplying both sides on the right by y.

(4) $\implies$ (2): The follows from writing (4) as $L_e L_x^{-1} L_e = L_{(e(x\backslash e))/(e\backslash e)}$ for all $x \in Q$. □

Left Bol loops have the LIP. On the other hand, if $(Q,+)$ is a loop such that every loop isotope has the LIP, then $(Q,+)$ is a left Bol loop. Left Bol loops are also nicely characterized by their left translations: a loop $(Q,+)$ is a left Bol loop if and only if, for all $x, y \in Q$, $L_x^+ L_y^+ L_x^+$ is a left translation.

Theorem 5.7. Let $(Q,\cdot)$ be a quasigroup. The following are equivalent.

1. $(Q,\cdot)$ is isotopic to a left Bol loop;

2. For each $u \in Q$, $(Q,+_u)$ has the LIP;

3. For all $x, y \in Q$, $L_x L_y^{-1} L_x$ is a left translation;

4. For all $x, y, z, v \in Q$, $x(y\backslash(xz)) = ((x(y\backslash(xv)))/v)z$;

5. For all $x, y, z \in Q$, $x(y\backslash(xz)) = ((x(y\backslash x))/(x\backslash x))z$.

Proof. (1) $\implies$ (2): By the discussion above, every loop isotopic to a left Bol loop has the LIP.

The equivalence of (2), (3), (4), (5) follows from Lemma 5.6.

(3) $\implies$ (1): Fix $u \in Q$ and consider the loop $(Q,+_u)$. For $x, y \in Q$, we compute

$$L_x^+ L_y^+ L_x^+ = L_{x/u} L_u^{-1} L_{y/u} L_u^{-1} L_{x/u} L_u^{-1},$$

$$
\begin{aligned}
&= L_{x/u}(L_u L_{y/u}^{-1} L_u)^{-1} L_{x/u} L_u^{-1}\,, & \\
&= L_{x/u} L_z^{-1} L_{x/u} L_u^{-1} & \text{for some } z \in Q\,, \\
&= L_w L_u^{-1} & \text{for some } w \in Q\,, \\
&= L^{+}_{wu}\,. &
\end{aligned}
$$

Thus $(Q, +_u)$ is a left Bol loop. □

Remark 5.8. It is tempting to refer to the variety of quasigroups with left Bol loop isotopes as simply being "left Bol quasigroups", and define them by, say, Theorem 5.7(4) or (5) or some other equivalent identity. However, the term "left Bol quasigroup" has already been used in at least two distinct ways in the literature.

D. Robinson [34] defined a right Bol quasigroup to be one which satisfies the right Bol identity and so by duality, a quasigroup $(Q, \cdot)$ is a left Bol quasigroup in Robinson's sense if it satisfies $x(y \cdot xz) = (x \cdot yx)z$ for all $x, y, z \in Q$.

Florja [14] defined a quasigroup $(Q, \cdot)$ to be a left Bol quasigroup if it satisfies the identity

$$x(y(xz)) = ((x(yx))/(x\backslash x))z \tag{5.2}$$

for all $x, y, z \in Q$ (see also [36], p. 109). Compare this with Theorem 5.7(5) which characterizes quasigroups with left Bol loop isotopes. It is easy to see that (5.2) is equivalent to the condition that for all $x, y \in Q$, $L_x L_y L_x$ is a left translation.

It is not difficult to show that a left Bol quasigroup in Robinson's sense is precisely the same as a left Bol quasigroup in Florja's sense with a right identity element. In addition, a left Bol quasigroup in Florja's sense is precisely the same as an LIP quasigroup with a left Bol loop isotope.

Lemma 5.6 and Theorem 5.7 have obvious right-handed duals which we will not state explicitly. Instead we pass directly to the two-sided case, which follows immediately. We will not use these results in the remainder of this chapter.

Lemma 5.9. Let $(Q, \cdot)$ be a quasigroup and fix $e \in Q$. The following are equivalent.

1. $(Q, +_e)$ is an IP loop;

2. For all $x \in Q$, $L_e L_x^{-1} L_e$ is a left translation and $R_e R_x^{-1} R_e$ is a right translation;

3. For all $x, y, z \in Q$,

$$(e(x\backslash(ey)))/y = (e(x\backslash(ez)))/z \qquad \text{and} \qquad y\backslash(((ye)/x)e) = z\backslash(((ze)/x)e)\,;$$

4. For all $x, y \in Q$,

$$e(x\backslash(ey)) = ((e(x\backslash e))/(e\backslash e))y \qquad \text{and} \qquad ((ye)/x)e = y((e/e)\backslash((e/x)e))\,.$$

Theorem 5.10. Let $(Q, \cdot)$ be a quasigroup. The following are equivalent.

1. $(Q, \cdot)$ is isotopic to a Moufang loop;

2. For each $u \in Q$, $(Q, +_u)$ has the IP;

3. For all $x, y \in Q$, $L_x L_y^{-1} L_x$ is a left translation and $R_x R_y^{-1} R_x$ is a right translation;

4. For all $x, y, z, v \in Q$,

$$x(y\backslash(xz)) = ((x(y\backslash(xv)))/v)z \quad \text{and} \quad ((zx)/y)x = z(v\backslash(((vx)/y)x))\,;$$

5. For all $x, y, z \in Q$,

$$x(y\backslash(xz)) = ((x(y\backslash x))/(x\backslash x))z \quad \text{and} \quad ((zx)/y)x = z((x/x)\backslash((x/y)x))\,.$$

5.3 Quasigroups isotopic to commutative Moufang loops

Our goal in this section is prove Theorem 5.2. We start by characterizing when the loop isotopes $(Q, +_e)$, $e \in Q$, are commutative.

Lemma 5.11. Let $(Q, \cdot)$ be a quasigroup and fix $e \in Q$. The following are equivalent.

1. $(Q, +_e)$ is commutative;
2. For all $x, y \in Q$, $x(e\backslash(ye)) = y(e\backslash(xe))$;
3. For all $x, y \in Q$, $((ey)/e)x = ((ex)/e)y$.

Proof. In terms of the quasigroup operations, commutativity of $+_e$ is given by

$$(x/e)(e\backslash y) = (y/e)(e\backslash x)\,.$$

Set $z = x/e$ so that $x = ze$, and set $v = y/e$ so that $y = ve$. Then $z(e\backslash(ve)) = v(e\backslash(ze))$. The steps are reversible, so (1) and (2) are equivalent. The equivalence of (1) and (3) is proved similarly. □

A loop $(Q, +)$ is said to have the *crossed inverse property* (CIP) if it satisfies either, and hence both, of the following identities for all $x, y \in Q$ [33]:

$$(-)_\lambda x + (y + x) = y \qquad \text{and} \qquad (x + y) + (-)_\rho x = y\,. \tag{CIP}$$

Here $(-)_\lambda x$ and $(-)_\rho x$ denote, respectively, the left and right inverses of $x \in (Q, +)$.

Lemma 5.12. Let $(Q, \cdot)$ be a quasigroup and fix $e \in Q$. The following are equivalent.

1. $(Q, +_e)$ has the CIP;
2. For all $x, y \in Q$, $((ee)/x)y = ((ey)/x)e$;
3. For all $x, y \in Q$, $x(y\backslash(ee)) = e(y\backslash(xe))$.

Proof. We write the leftmost identity in (CIP) in terms of the quasigroup operations:

$$[(ee)/(e\backslash x)][e\backslash((y/e)(e\backslash x))] = y\,. \tag{5.3}$$

Set $v = e\backslash x$ so that $x = ev$, and set $w = e\backslash((y/e)v)$ so that $y = ((ew)/v)e$. Then (5.3) is equivalent to

$$((ee)/v)w = ((ew)/v)e\,. \tag{5.4}$$

Thus parts (1) and (2) are equivalent. A dual argument using the rightmost identity of (CIP) yields the equivalence of (1) and (3). □

Corollary 5.13. The identities (Q1) and (Q2) are equivalent in quasigroups.

Lemma 5.14. Let $(Q, \cdot)$ be a quasigroup satisfying (Q1) and (Q2). Then for each x, y, z, u in Q, the following identities hold:

$$((xy)/x)z = ((xz)/x)y\,, \tag{5.5}$$

$$z(x\backslash(yx)) = y(x\backslash(zx))\,. \tag{5.6}$$

Proof. Starting with the left side of 5.5, we compute

$$\begin{aligned} ((xy)/x)z &= ((xy)/x)[((xx)/z)\backslash(xx)] \\ &= x[((xx)/z)\backslash\underbrace{(((xy)/x)x)}_{}] \end{aligned} \tag{Q1}$$

$$
\begin{aligned}
&= x[((xx)/z)\backslash(xy)] \\
&= x\{y\backslash(\underbrace{y[((xx)/z)\backslash(xy)]})\} \\
&= x\{y\backslash(x[((xx)/z)\backslash\underbrace{(yy)}])\} && \text{(Q1)} \\
&= x\{y\backslash(\underbrace{x[((xx)/z)\backslash(((yy)/x)x)]})\} \\
&= x\{y\backslash(((yy)/x)[\underbrace{((xx)/z)\backslash(xx)}])\} && \text{(Q1)} \\
&= x\{y\backslash(((yy)/x)z)\}\,.
\end{aligned}
$$

Reversing the roles of y and z in this calculation, we see that (5.5) is equivalent to the identity $x\{y\backslash(((yy)/x)z)\} = x\{z\backslash(((zz)/x)y)\}$, or just

$$
y\backslash(((yy)/x)z) = z\backslash(((zz)/x)y)\,. \tag{5.7}
$$

To prove (5.7), we start with its left side and compute

$$
\begin{aligned}
y\backslash(((yy)/x)z) &= z\backslash\{\underbrace{z[y\backslash(((yy)/x)z)]}\} \\
&= z\backslash\{\underbrace{((yy)/x)[y\backslash(zz)]}\} && \text{(Q1)} \\
&= z\backslash\{((\underbrace{y(y\backslash(zz))})/x)y\} && \text{(Q2)} \\
&= z\backslash(((zz)/x)y)\,.
\end{aligned}
$$

This completes the proof of (5.5) and the proof of (5.6) is dual to this. □

Corollary 5.15. If $(Q,\cdot)$ is a quasigroup satisfying (Q1) and (Q2), then for each $u \in Q$, $(Q,+_u)$ is commutative.

Proof. This follows immediately from Lemmas 5.14 and 5.11. □

We are now equipped to prove Theorem 5.2, which for convenience is restated here.

Theorem 5.2. Let $(Q, \cdot)$ be a quasigroup. The following are equivalent:

1. Each loop isotope $(Q, +_u)$ is a commutative Moufang loop.
2. For all $x, y, z \in Q$, the following identity holds:
$$x(y\backslash(zz)) = z(y\backslash(xz))\,. \tag{Q1}$$
3. For all $x, y, z \in Q$, the following identity holds:
$$((zz)/y)x = ((zx)/y)z\,. \tag{Q2}$$

Proof. Commutative Moufang loops have the CIP, so if part (1) of the theorem holds, then every $(Q, +_u)$ has the CIP, and so Lemma 5.12 implies parts (2) and (3).

By Corollary 5.13, (Q1) and (Q2) are equivalent, so we may assume both parts (2) and (3) hold. By Corollary 5.15, each $(Q, +_u)$ is commutative. What remains is to show that each $(Q, +_u)$ is a Moufang loop. By commutativity, it is sufficient to show that each $(Q, +_u)$ is a left Bol loop. Thus for $x, y, z \in Q$, we compute

$$\begin{aligned} L_x L_y^{-1} L_x(z) &= x(y\backslash(xz)) \\ &= x(y\backslash([(xz)/x]x)) \\ &= [(xz)/x](y\backslash(xx)) && \text{(Q1)} \\ &= [(x(y\backslash(xx)))/x]z && \text{(5.6)} \\ &= L_{(x(y\backslash(xx)))/x}(z)\,. \end{aligned}$$

Thus for all $x, y \in Q$, $L_x L_y^{-1} L_x$ is a left translation. An application of Theorem 5.7 completes the proof. □

5.4 Semiparamedial quasigroups

Having an understanding of the loop isotopes of a quasigroup can be helpful, but being able to represent a variety of quasigroups as affine over a structured class of loops is better. Thus, in this section, our goal is to prove Theorem 5.5. We begin by showing that both semimedial and semiparamedial quasigroups satisfy (Q1).

Recall that a semiparamedial quasigroup $(Q, \cdot)$ is a quasigroup satisfying the following for all $x, y, z \in Q$:

$$xx \cdot yz = zx \cdot yx\,, \tag{P1}$$

$$xy \cdot zz = zy \cdot zx\,. \tag{P2}$$

We introduce one more identity in a quasigroup $(Q, \cdot)$: for every $x, y, z \in Q$:

$$xy \cdot yz = zy \cdot yx\,. \tag{P3}$$

Lemma 5.16. Let $(Q, \cdot)$ be a quasigroup. If $(Q, \cdot)$ is semimedial or semiparamedial, then $(Q, \cdot)$ satisfies (Q1).

Proof. Assume first that $(Q, \cdot)$ is semimedial and fix $x, y, z \in Q$. Then:

$$\begin{aligned} yy \cdot x(y\backslash(zz)) &= yx \cdot y(y\backslash(zz)) && \text{(S1)} \\ &= yx \cdot zz \\ &= yz \cdot xz && \text{(S2)} \\ &= yz \cdot y(y\backslash(xz)) \\ &= yy \cdot z(y\backslash(xz))\,. && \text{(S1)} \end{aligned}$$

Canceling yy, we have (Q1).

Next assume $(Q,\cdot)$ is semiparamedial and fix $x,y,z\in Q$. Then:

$$\begin{aligned}
x(y\backslash(zz))\cdot yy &= y(y\backslash(zz))\cdot yx && \text{(P2)}\\
&= zz\cdot yx\\
&= xz\cdot yz && \text{(P1)}\\
&= y(y\backslash(xz))\cdot yz\\
&= z(y\backslash(xz))\cdot yy\,. && \text{(P2)}
\end{aligned}$$

Canceling yy, we have (Q1). □

We will need part of the following result in our affine characterization of semiparamedial quasigroups.

Proposition 5.17. In a cancellative magma $(Q,\cdot)$, any two of (P1), (P2), or (P3) together imply the third.

Proof. We show first that (P1) and (P2) together imply (P3). For $x,y,z\in Q$, we have:

$$\begin{aligned}
(xy\cdot xy)(zz\cdot xz)\cdot\underbrace{(xx\cdot xy)(zx\cdot xy)} &= (xy\cdot xy)(zz\cdot xz)\cdot(xy\cdot xy)\underbrace{(zx\cdot xx)} && \text{(P1)}\\
&= (xy\cdot xy)(zz\cdot xz)\cdot(xy\cdot xy)(xx\cdot xz) && \text{(P2)}\\
&= \underbrace{(xx\cdot xz)(zz\cdot xz)}\cdot(xy\cdot xy)(xy\cdot xy) && \text{(P2)}\\
&= (xz\cdot xz)\underbrace{(zz\cdot xx)}\cdot(xy\cdot xy)(xy\cdot xy) && \text{(P1)}\\
&= (xz\cdot xz)(xz\cdot xz)\cdot\underbrace{(xy\cdot xy)}\underbrace{(xy\cdot xy)} && \text{(P1)}\\
&= (xz\cdot xz)(xz\cdot xz)\cdot\underbrace{(yy\cdot xx)(yy\cdot xx)} && \text{(P1)}\\
&= (xz\cdot xz)(xz\cdot xz)\cdot(xx\cdot xx)(yy\cdot yy) && \text{(P1)}\\
&= \underbrace{(yy\cdot yy)(xz\cdot xz)}\cdot\underbrace{(xx\cdot xx)(xz\cdot xz)} && \text{(P1)}
\end{aligned}$$

$$= \underbrace{(xz \cdot yy)}_{}\,\underbrace{(xz \cdot yy)}_{} \cdot (xz \cdot xx)(xz \cdot xx) \qquad \text{(P1)}$$

$$= \underbrace{(yz \cdot yx)(yz \cdot yx)}_{} \cdot (xz \cdot xx)(xz \cdot xx) \qquad \text{(P2)}$$

$$= (yx \cdot yx)(yz \cdot yz) \cdot (xz \cdot xx)(xz \cdot xx) \qquad \text{(P1)}$$

$$= \underbrace{(xz \cdot xx)(yz \cdot yz)}_{} \cdot \underbrace{(xz \cdot xx)(yx \cdot yx)}_{} \qquad \text{(P2)}$$

$$= \underbrace{(yz \cdot xx)}_{}(yz \cdot xz) \cdot \underbrace{(yx \cdot xx)}_{}(yx \cdot xz) \qquad \text{(P2)}$$

$$= (xz \cdot xy)\,\underbrace{(yz \cdot xz)}_{} \cdot (xx \cdot xy)(yx \cdot xz) \qquad \text{(P2)}$$

$$= \underbrace{(xz \cdot xy)(zz \cdot xy)}_{} \cdot (xx \cdot xy)(yx \cdot xz) \qquad \text{(P1)}$$

$$= (xy \cdot xy)(zz \cdot xz) \cdot (xx \cdot xy)(yx \cdot xz)\,. \qquad \text{(P1)}$$

Thus $(xy \cdot xy)(zz \cdot xz) \cdot (xx \cdot xy)(zx \cdot xy) = (xy \cdot xy)(zz \cdot xz) \cdot (xx \cdot xy)(yx \cdot xz)$. Canceling $(xy \cdot xy)(zz \cdot xz)$ on the left, we get $(xx \cdot xy)(zx \cdot xy) = (xx \cdot xy)(yx \cdot xz)$, and then canceling $xx \cdot xy$, we obtain the desired result: $zx \cdot xy = yx \cdot xz$.

Next assume (P1) and (P3) hold. Then for all $x, y, z \in Q$,

$$\underbrace{(xy \cdot zz)(zz \cdot zz)}_{} \cdot (zx \cdot zz)(zz \cdot xz) = (zz \cdot zz)\,\underbrace{(zz \cdot xy)}_{} \cdot (zx \cdot zz)(zz \cdot xz) \qquad \text{(P3)}$$

$$= \underbrace{(zz \cdot zz)(yz \cdot xz)}_{} \cdot (zx \cdot zz)(zz \cdot xz) \qquad \text{(P1)}$$

$$= (xz \cdot zz)\,\underbrace{(yz \cdot zz)}_{} \cdot (zx \cdot zz)(zz \cdot xz) \qquad \text{(P1)}$$

$$= \underbrace{(xz \cdot zz)(zz \cdot zy)}_{} \cdot (zx \cdot zz)(zz \cdot xz) \qquad \text{(P3)}$$

$$= (zy \cdot zz)(zz \cdot xz) \cdot (zx \cdot zz)(zz \cdot xz) \qquad \text{(P3)}$$

$$= \underbrace{(zz \cdot xz)(zz \cdot xz)}_{} \cdot \underbrace{(zx \cdot zz)(zy \cdot zz)}_{} \qquad \text{(P1)}$$

$$= (xz \cdot xz)(zz \cdot zz) \cdot (zz \cdot zz)(zy \cdot zx) \qquad \text{(P1)}$$

$$= (zy \cdot zx)(zz \cdot zz) \cdot \underbrace{(zz \cdot zz)(xz \cdot xz)}_{} \qquad \text{(P3)}$$

$$
\begin{aligned}
&= (zy \cdot zx)(zz \cdot zz) \cdot (xz \cdot zz)\underbrace{(xz \cdot zz)} && \text{(P1)}\\
&= (zy \cdot zx)(zz \cdot zz) \cdot \underbrace{(xz \cdot zz)(zz \cdot zx)} && \text{(P3)}\\
&= (zy \cdot zx)(zz \cdot zz) \cdot (zx \cdot zz)(zz \cdot xz)\,. && \text{(P3)}
\end{aligned}
$$

Thus, $(xy \cdot zz)(zz \cdot zz) \cdot (zx \cdot zz)(zz \cdot xz) = (zy \cdot zx)(zz \cdot zz) \cdot (zx \cdot zz)(zz \cdot xz)$. Applying cancellation twice yields the desired result, $xy \cdot zz = zy \cdot zx$.

Finally, if (P2) and (P3) hold in $(Q, \cdot)$, then (P1) and (P3) hold in the opposite cancellative magma $(Q, *)$ where $x * y = y \cdot x$. By the preceding case, (P2) holds in $(Q, *)$, which is equivalent to (P1) holding in $(Q, \cdot)$. This completes the proof. □

It can be useful at times to think of the quasigroup operations in terms of its left and right translation maps, which is why we state and prove the following.

Lemma 5.18. For a semiparamedial quasigroup $(Q, \cdot)$ and for all $x, y, a, b \in Q$:

(i) $L_{xx}R_y = L_{yx}R_x$, $R_{yy}L_x = R_{yx}L_y$, $L_{xx}L_x = R_{xx}R_x$, and $L_{xy}L_y = R_{yx}R_y$;

(ii) $L_{xx}(ab) = R_x(b)R_x(a)$, and $L_{xx}^{-1}(ab) = R_x^{-1}(b)R_x^{-1}(a)$.

Proof. Let $x, y, z, a, b \in Q$. For (i), we have $L_{xx}R_y(z) = (xx)(zy) = (yx)(zx)$ by (P1). Notice $(yx)(zx) = L_{yx}R_x(z)$. Further, $R_{yy}L_x(z) = (xz)(yy) = (yz)(yx)$ by (P2). Notice $(yz)(yx) = R_{yx}L_y(z)$. Moreover, $L_{xx}L_x(z) = (xx)(xz) = (zx)(xx)$ by (P1). Notice $(zx)(xx) = R_{xx}R_x(z)$. Lastly, $L_{xy}L_y(z) = (xy)(yz) = (zy)(yx)$ by Lemma 5.17. Notice $(zy)(yx) = R_{yx}R_y(z)$.

Now for (ii), we have $L_{xx}(ab) = (xx)(ab) = (bx)(ax)$ by (P1), and $(bx)(ax) = R_x(b) \cdot R_x(a)$. In addition, $L_{xx}^{-1}(ab) = R_x^{-1}(b) \cdot R_x^{-1}(a)$ if and only if $(xx)\backslash(ab) = b/x \cdot a/x$. Multiplying both sides by xx, we see this is equivalent to $ab = (xx)(b/x \cdot a/x)$. Then an application of (P1) gives that this is true if and only if $ab = ((a/x) \cdot x)((b/x) \cdot x)$. Reducing we see that $L_{xx}^{-1}(ab) = R_x^{-1}(b) \cdot R_x^{-1}(a)$ holds if and only if $ab = ab$, which is certainly true.

Thus, all of the equations in Lemma 5.18 hold. □

Before the proof of Theorem 5.5, it is necessary to define some terms and set up a few more preliminary results, which is what we will do now. Let $(Q, \cdot)$ be a quasigroup and fix $e \in Q$. We define a new map on Q by $\alpha := R_e \cdot L_e^{-1}$. Let $+ = +_e$ be defined as usual. We will say $(Q, +)$ has the property (A1) if, for every $x, y, z \in Q$, the following equation holds:

$$(\alpha(x) + x) + (y + z) = (\alpha(x) + y) + (x + z). \tag{A1}$$

It is our goal now to show that if $(Q, \cdot)$ is a semiparamedial quasigroup, then Q satisfies (A1). To do this, we will use the following fact about commutative Moufang loops, stated as Lemma VII.5.7. in [6].

Lemma 5.19. Let $(Q, +)$ be a commutative Moufang loop and $x \in Q$. Then $3x \in Z(Q)$.

Theorem 5.20. Let Q be a quasigroup satisfying (Q1), fix $e \in Q$, and let $(Q, +)$ be the associated commutative Moufang loop where $+ = +_e$. Then (A1) holds.

Proof. First observe that

$$\alpha(x) + x = (e\backslash x)^2 \tag{5.8}$$

for all $x \in Q$, as is immediate from the definition of α.

We will also need the following:

$$x + -y = (x/(e\backslash y))e \tag{5.9}$$

for all $x, y \in Q$. Indeed, the right inverse property is $x = (x + -y) + y = (x + -y)/e \cdot e\backslash y$, and solving this for $x + -y$ gives (5.9).

Similarly, we have

$$e\backslash(x+y) = (-x/e)\backslash y \tag{5.10}$$

for all $x, y \in Q$, which follows from the left inverse property.

Now we prove

$$((\alpha(x)+x)+y)+z = \alpha(x)+(y+(x+z)) \tag{5.11}$$

for all $x, y, z \in Q$. We compute

$$\begin{aligned}
((\alpha(x)+x)+y)+z &= ((z+x)+-x)+(y+(\alpha(x)+x)) \\
&= ((z+x)/(e\backslash x))e \cdot (e\backslash(y+(e\backslash x)^2)) && (5.9), (5.8) \\
&= ((z+x)/(e\backslash x))e \cdot ((-y/e)\backslash(e\backslash x)^2) && (5.10) \\
&= (e\backslash x) \cdot ((-y/e)\backslash[((z+x)/(e\backslash x))(e\backslash x)]) && \text{(Q2)} \\
&= (e\backslash x) \cdot ((-y/e)\backslash(z+x)) \\
&= (\alpha(x)/e)(e\backslash(y+(z+x))) && (5.10) \\
&= \alpha(x)+(y+(x+z))\,.
\end{aligned}$$

Next, we add y to both sides of (5.11). On the left side, we get

$$(((\alpha(x)+x)+y)+z)+y = (\alpha(x)+x)+(y+z+y) = (\alpha(x)+x)+(2y+z)\,,$$

using a Moufang identity. On the right side, we similarly compute

$$y+(\alpha(x)+(y+(x+z))) = (y+\alpha(x)+y)+(x+z) = (\alpha(x)+2y)+(x+z)\,.$$

Putting these together and replacing y with $-y$, we have

$$(\alpha(x)+x)+(-2y+z)=(\alpha(x)+-2y)+(x+z) \tag{5.12}$$

for all $x,y,z\in Q$. Now in (5.12), rewrite $-2y=y+-3y$. By Lemma 5.19, $-3y$ is in the center of $(Q,+)$. Thus we may cancel $-3y$ from both sides of the rewritten (5.12) to obtain

$$(\alpha(x)+x)+(y+z)=(\alpha(x)+y)+(x+z)$$

for all $x,y,z\in Q$. Therefore (A1) holds as claimed. □

The following is an immediate consequence of Corollary 5.13, Lemma 5.16, and Theorem 5.20.

Corollary 5.21. Let $(Q,\cdot)$ be a semiparamedial quasigroup. Fix $x\in Q$. Let $(Q,+)$ be the CML defined by $+=+_{xx}$ and let $e=xx$ in the definition of α. Then $(Q,+)$ satisfies (A1).

Lemma 5.22. Let $(Q,\cdot)$ be a semiparamedial quasigroup and let $a,b\in Q$. Then α is an automorphism of the CML isotope $(Q,+)$, with $+=+_{xx}$, as defined above.

Proof. Let $(Q,\cdot)$, α, and $+$ be as defined, and let $a,b\in Q$. Then:

$$\begin{align*}
\alpha(a+b) &= R_{xx}L_{xx}^{-1}(a+b)\\
&= R_{xx}L_{xx}^{-1}(R_{xx}^{-1}(a)\cdot L_{xx}^{-1}(b))\\
&= R_{xx}(R_x^{-1}L_{xx}^{-1}(b)\cdot R_x^{-1}R_{xx}^{-1}(a)) \tag*{5.18}\\
&= L_xR_x^{-1}R_{xx}^{-1}(a)\cdot L_xR_x^{-1}L_{xx}^{-1}(b) \tag*{5.18}\\
&= L_xL_x^{-1}L_{xx}^{-1}(a)\cdot L_xR_x^{-1}L_{xx}^{-1}(b) \tag*{5.18}\\
&= L_{xx}^{-1}(a)\cdot L_xR_x^{-1}L_{xx}^{-1}(b)\\
&= L_{xx}^{-1}(a)\cdot L_{xx}^{-1}R_{xx}R_xR_x^{-1}L_{xx}^{-1}(b) \tag*{5.18}
\end{align*}$$

$$\begin{aligned}
&= L_{xx}^{-1}(a) \cdot L_{xx}^{-1} R_{xx} L_{xx}^{-1}(b) \\
&= R_{xx}^{-1} R_{xx} L_{xx}^{-1}(a) \cdot L_{xx}^{-1} R_{xx} L_{xx}^{-1}(b) \\
&= R_{xx}^{-1}(\alpha(a)) \cdot L_{xx}^{-1}(\alpha(b)) \\
&= \alpha(a) + \alpha(b).
\end{aligned}$$

Thus, α is an automorphism of $(Q, +)$. □

Sometimes automorphisms of loops can have special properties which lend to the structure of the loop. One such we define below.

Definition 5.4. Let α be a map on a loop $(Q, +)$. Then α is called *nuclear* if, for every $x \in Q$, $-x + \alpha(x) \in N(Q)$.

Analogous to Kepka's result in the semimedial case, we can now formulate and prove the following theorem for semiparamedial quasigroups.

Theorem 5.5. Let $(Q, \cdot)$ be a quasigroup. Then $(Q, \cdot)$ is semiparamedial if and only if $(Q, \cdot)$ has affine form $(Q, +, \psi, \varphi, g)$ where $(Q, +)$ is a commutative Moufang loop, $\varphi^2 = \psi^2$, and $\psi\varphi^{-1}$ is a nuclear automorphism of $(Q, +)$.

Proof. $(\Rightarrow)$ Fix $x \in Q$. Let $y := xx$ and $0 := yy$. Define $a + b = R_y^{-1}(a) L_y^{-1}(b)$. By Lemma 5.16 together with Theorem 5.2, $(Q, +)$ is a commutative Moufang loop with unit 0 satisfying (A1) for $\alpha = R_y L_y^{-1}$. Moreover, by Proposition 4.2 in [21], α is a nuclear mapping of $(Q, +)$.

By Lemma 5.18, we can write:

$$\begin{aligned}
L_y(a + b) &= L_y(R_y^{-1}(a) \cdot L_y^{-1}(b)) \\
&= R_x R_y^{-1}(a) \cdot R_x L_y^{-1}(b) \\
&= R_y^{-1} R_y R_x R_y^{-1}(a) \cdot L_y^{-1} L_y R_x L_y^{-1}(b)
\end{aligned}$$

$$= R_y R_x R_y^{-1}(a) + L_y R_x L_y^{-1}(b).$$

Now consider $L_y(a) = L_y(a+0) = R_y R_x R_y^{-1}(a) + L_y R_x L_y^{-1}(0)$ and $L_y(b) = L_y(0+b) = R_y R_x R_y^{-1}(0) + L_y R_x L_y^{-1}(b)$. Since $(Q,+)$ is commutative and has the inverse property, we may then write $L_y(a+b) = R_y R_x R_y^{-1}(a) + L_y R_x L_y^{-1}(b) = (L_y(a) + -L_y R_x L_y^{-1}(0)) + (L_y(b) + -R_y R_x R_y^{-1}(0))$.

Notice $\alpha(L_y R_x L_y^{-1}(0)) = R_y L_y^{-1} L_y R_x L_y^{-1}(0) = R_y R_x(y) = R_y R_x R_y^{-1}(0)$, and since α is an automorphism of $(Q,+)$, it follows that $\alpha(-L_y R_x L_y^{-1}(0)) = -R_y R_x R_y^{-1}(0)$. Thus,

$$\begin{aligned}
&L_y(a+b)\\
&\quad = (L_y(a) + -L_y R_x L_y^{-1}(0)) + (L_y(b) + -R_y R_x R_y^{-1}(0))\\
&\quad = (L_y(a) + -L_y R_x L_y^{-1}(0)) + (L_y(b) + \alpha(-L_y R_x L_y^{-1}(0))\\
&\quad = (\alpha(-L_y R_x L_y^{-1}(0)) + L_y(b)) + (-L_y R_x L_y^{-1}(0) + L_y(a)) && \text{(commutativity)}\\
&\quad = (\alpha(-L_y R_x L_y^{-1}(0)) + -L_y R_x L_y^{-1}(0)) + (L_y(b) + L_y(a)) && \text{(A1)}\\
&\quad = (L_y(b) + L_y(a)) + (-R_y R_x R_y^{-1}(0) + -L_y R_x L_y^{-1}(0)) && \text{(commutativity).}
\end{aligned}$$

Define $k := L_y R_x L_y^{-1}(0) + R_y R_x R_y^{-1}(0)$ and $\varphi(a) := L_y(a) + -k$.

We claim now that φ is an automorphism of $(Q,+)$. To see this, let $a, b \in Q$. Then we have the following:

$$\begin{aligned}
\varphi(a+b) &= L_y(a+b) + -k\\
&= ((L_y(a) + L_y(b)) + -k) + -k\\
&= (L_y(a) + L_y(b)) + (-k + -k) && \text{(Moufang)}\\
&= (L_y(a) + -k) + (L_y(b) + -k) && \text{(CML)}\\
&= \varphi(a) + \varphi(b).
\end{aligned}$$

Moreover, we have that $L_y(0) = L_y(0+0) = (L_y(0) + L_y(0)) + -k$. Since Moufang loops have the inverse property, we may use this along with cancellation to obtain $k = L_y(0)$. Thus, $\varphi(a) = L_y(a) + -L_y(0)$.

Similarly, using the right translation map and by Lemma 5.18, we may write:

$$\begin{aligned}
R_y(a+b) &= R_y(R_y^{-1}(a) \cdot L_y^{-1}(b)) \\
&= L_x R_y^{-1}(a) \cdot L_x L_y^{-1}(b) \\
&= R_y^{-1} R_y L_x R_y^{-1}(a) \cdot L_y^{-1} L_y L_x L_y^{-1}(b) \\
&= R_y L_x R_y^{-1}(a) + L_y L_x L_y^{-1}(b).
\end{aligned}$$

Now consider $R_y(a) = R_y(a+0) = R_y L_x R_y^{-1}(a) + L_y L_x L_y^{-1}(0)$ and $R_y(b) = R_y(0+b) = R_y L_x R_y^{-1}(0) + L_y L_x L_y^{-1}(b)$. Again, because $(Q,+)$ is commutative and has the inverse property, we may write $R_y(a+b) = R_y L_x R_y^{-1}(a) + L_y L_x L_y^{-1}(b) = (R_y(a) + -L_y L_x L_y^{-1}(0)) + (R_y(b) + -R_y L_x R_y^{-1}(0))$.

Notice

$$\alpha(L_y L_x L_y^{-1}(0)) = R_y L_y^{-1} L_y L_x L_y^{-1}(0) = R_y L_x L_y^{-1}(0) = R_y L_x(y) = R_y L_x R_y^{-1}(0)$$

and since α is an automorphism of $(Q,+)$, it follows that

$$\alpha(-L_y L_x L_y^{-1}(0)) = -R_y L_x R_y^{-1}(0)\,.$$

Thus,

$$\begin{aligned}
&R_y(a+b) \\
&\quad = (R_y(a) + -L_y L_x L_y^{-1}(0)) + (R_y(b) + -R_y L_x R_y^{-1}(0))
\end{aligned}$$

$$
\begin{aligned}
&= (R_y(a) + -L_yL_xL_y^{-1}(0)) + (R_y(b) + \alpha(-L_yL_xL_y^{-1}(0))) \\
&= (\alpha(-L_yL_xL_y^{-1}(0)) + R_y(b)) + (-L_yL_xL_y^{-1}(0) + R_y(a)) && \text{(commutativity)} \\
&= (\alpha(-L_yL_xL_y^{-1}(0)) + -L_yL_xL_y^{-1}(0)) + (R_y(b) + R_y(a)) && \text{(A1)} \\
&= (R_y(a) + R_y(b)) + (-R_yL_xR_y^{-1}(0) + -L_yL_xL_y^{-1}(0))\,. && \text{(commutativity)}
\end{aligned}
$$

Define $l := L_yL_xL_y^{-1}(0) + R_yL_xR_y^{-1}(0)$ and $\psi(a) := R_y(a) + -l$.

We claim that ψ is an automorphism of $(Q, +)$. Let $a, b \in Q$, then

$$
\begin{aligned}
\psi(a+b) &= R_y(a+b) + -l \\
&= ((R_y(a) + R_y(b)) + -l) + -l \\
&= (R_y(a) + R_y(b)) + (-l + -l) && \text{(Moufang)} \\
&= (R_y(a) + -l) + (R_y(b) + -l) && \text{(CML)} \\
&= \psi(a) + \psi(b)\,.
\end{aligned}
$$

Notice $R_y(0) = R_y(0+0) = (R_y(0) + R_y(0)) + -l$. Again, the inverse property and cancellation give that $l = R_y(0)$, so $\psi(a) = R_y(a) + -R_y(0)$. Moreover, $\alpha(k) = R_yL_y^{-1}L_y(0) = R_y(0) = l$.

So we have

$$
\begin{aligned}
a \cdot b &= R_y(a) + L_y(b) \\
&= (\psi(a) + l) + (\varphi(b) + k) \\
&= (\psi(a) + \alpha(k)) + (\varphi(b) + k) \\
&= (\psi(a) + \varphi(b)) + (\alpha(k) + k)\,.
\end{aligned}
$$

By letting $g := \alpha(k) + k$, we have the property desired.

Since $\varphi(a) = L_y(a) + -k$ for every $a \in Q$, we have that $\varphi^{-1}(a) = L_y^{-1}(a+k)$, so

$$\begin{aligned}
\psi\varphi^{-1}(a) &= \psi L_y^{-1}(a+k) \\
&= R_y L_y^{-1}(a+k) + -l \\
&= R_y L_y^{-1}(a+k) + -\alpha(k) \\
&= \alpha(a+k) + -\alpha(k) \\
&= (\alpha(a) + \alpha(k)) + -\alpha(k) \\
&= \alpha(a)\,.
\end{aligned}$$

Since this is true for every $a \in Q$, we have that $\psi\varphi^{-1} = \alpha$, and since α is a nuclear mapping of $(Q,+)$, so is $\psi\varphi^{-1}$.

Lastly, we show that $\varphi^2 = \psi^2$. First we will need the following lemmas.

Lemma 5.23. In this setting and for every $a \in Q$, $\psi(a) = a \cdot (0\backslash 0)$.

Proof. First, note the following:

$$\begin{aligned}
0/(e\backslash\psi(e)) &= 0/(e\backslash(0 + -(0\cdot e))) \\
&= 0/(e\backslash -(0\cdot e)) \\
&= ((0\cdot e) + -(0\cdot e))/(e\backslash -(0\cdot e)) \\
&= (((0\cdot e)/e)(e\backslash -(0\cdot e)))/(e\backslash -(0\cdot e)) \\
&= (0\cdot e)/e \\
&= 0\,.
\end{aligned}$$

Thus, it follows that $e\backslash\psi(e) = 0\backslash 0$, so we have $\psi(a) = (ae) + -(0e) = (ae) + (0 + -(0e)) = (ae) + \psi(e) = a(e\backslash\psi(e)) = a(0\backslash 0)$ by the argument above. □

Similarly, we have the following result for φ:

Lemma 5.24. In this setting and for every $a \in Q$, $\varphi(a) = (0/0) \cdot a$.

Proof. First, note the following:

$$\begin{aligned}
(\varphi(e)/e)\backslash 0 &= (-(e \cdot 0)/e)\backslash 0 \\
&= (-(e \cdot 0)/e)\backslash(-(e \cdot 0) + (e \cdot 0)) \\
&= (-(e \cdot 0)/e)\backslash((-(e \cdot 0)/e)(e\backslash(e \cdot 0))) \\
&= e\backslash(e \cdot 0)\,.
\end{aligned}$$

So it follows that $\varphi(e)/e = 0/0$, and thus we have $\varphi(a) = (ea) + -(e0) = (ea) + (0 + -(e0)) = (ea) + \varphi(e) = \varphi(e) + (ea) = (\varphi(e)/e)a = (0/0)a$. □

A result that will be useful is as follows:

Lemma 5.25. In this setting and for every $a, b \in Q$, the identity $0 \cdot (a + (0\backslash b)) = (b/0) \cdot a$ holds.

Proof. Let $a, b \in Q$. Then calculating, we have:

$$\begin{aligned}
(b/0) \cdot a &= [(0 \cdot (0\backslash b))/0] \cdot a \\
&= [(0 \cdot (e \cdot (e\backslash(0\backslash b))))/0] \cdot a \\
&= [((e \cdot e) \cdot (e \cdot (e\backslash(0\backslash b))))/0] \cdot a \\
&= [(((e\backslash(0\backslash b)) \cdot e) \cdot 0)/0] \cdot a && \text{(P1)} \\
&= [(e\backslash(0\backslash b)) \cdot e] \cdot a \\
&= [(e\backslash(0\backslash b)) \cdot e] \cdot [(a/e) \cdot e] \\
&= 0 \cdot [(a/e) \cdot (e\backslash(0\backslash b))] && \text{(P1)} \\
&= 0 \cdot (a + (0\backslash b))\,.
\end{aligned}$$

□

As a final lemma, we have the following:

Lemma 5.26. In this setting and for every $x, y \in Q$, the following identity holds: $0 \cdot (\varphi(x) + y) = \psi(x) \cdot y$.

Proof. Notice first that

$$\begin{aligned}
((e\backslash\varphi(x)) \cdot e) \cdot 0 &= 0 \cdot (e \cdot (e\backslash\varphi(x))) && \textbf{(P2)} \\
&= 0 \cdot \varphi(x) \\
&= 0 \cdot ((e \cdot x) + -(e \cdot 0)) \\
&= 0 \cdot (-(e \cdot 0) + (e \cdot x)) \\
&= 0 \cdot [(-(e \cdot 0)/e) \cdot (e\backslash(e \cdot x))] \\
&= 0 \cdot [(-(e \cdot 0)/e) \cdot x] \\
&= (x \cdot e) \cdot ((-(e \cdot 0)/e) \cdot e) && \textbf{(P1)} \\
&= (x \cdot e) \cdot (-(e \cdot 0)) \\
&= (x \cdot e) \cdot (0 + -(e \cdot 0)) \\
&= (x \cdot e) \cdot \varphi(e) \\
&= (x \cdot e) \cdot (e \cdot (e\backslash\varphi(e))) \\
&= ((e\backslash\varphi(e)) \cdot e) \cdot (e \cdot x) \,. && \textbf{(P3)}
\end{aligned}$$

Now $0 = x + -x$ holds if and only if $0 = (x/e) \cdot (e\backslash - x)$, which is true if and only if $(x/e)\backslash 0 = e\backslash - x$. Moreover, $0 \cdot x = (e \cdot e) \cdot (y \cdot (y\backslash x)) = ((y\backslash x) \cdot e) \cdot (y \cdot e)$ by (P1). Thus, $(0 \cdot x)/(y \cdot e) = (y\backslash x) \cdot e$. These together give us that $(e\backslash - x) \cdot e = ((x/e)\backslash 0) \cdot e =$

$(0 \cdot 0)/((x/e) \cdot e) = (0 \cdot 0)/x$. So

$$(e\backslash -x) \cdot e = (0 \cdot 0)/x. \tag{5.13}$$

Moreover, we have that $(x \cdot 0)/-\varphi(e) = ((0 \cdot (0\backslash x)) \cdot (e \cdot e))/(e \cdot 0) = ((e \cdot (0\backslash x)) \cdot (e \cdot 0))/(e \cdot 0) = e \cdot (0\backslash x)$. Thus, for any x,

$$(x \cdot 0)/-\varphi(e) = e \cdot (0\backslash x). \tag{5.14}$$

By the above arguments, we have

$$\begin{aligned}
((e\backslash\varphi(x)) \cdot e) \cdot 0 &= ((e\backslash\varphi(e)) \cdot e) \cdot (e \cdot x) \\
&= ((0 \cdot 0)/-\varphi(e)) \cdot (e \cdot x) && (5.13) \\
&= (e \cdot (0\backslash 0)) \cdot (e \cdot x) && (5.14) \\
&= (x \cdot (0\backslash 0)) \cdot 0 && \text{(P2)} \\
&= \psi(x) \cdot 0. && 5.23
\end{aligned}$$

Thus,

$$(e\backslash\varphi(x)) \cdot e = \psi(x). \tag{5.15}$$

Now,

$$\begin{aligned}
\psi(x) \cdot y &= ((e\backslash\varphi(x)) \cdot e) \cdot y && (5.15) \\
&= ((e\backslash\varphi(x)) \cdot e) \cdot ((y/e) \cdot e) \\
&= (e \cdot e) \cdot ((y/e) \cdot (e\backslash\varphi(x))) && \text{(P1)} \\
&= 0 \cdot (y + \varphi(x))
\end{aligned}$$

$$= 0 \cdot (\varphi(x) + y).$$

□

We are now equipped to finish the proof of the claim that $\varphi^2 = \psi^2$. Let $x \in Q$, then:

$$\begin{aligned}
\psi(\psi(x)) &= \psi(x \cdot (0\backslash 0)) && 5.23\\
&= (x \cdot (0\backslash 0)) \cdot (0\backslash 0) && 5.23\\
&= 0 \cdot (\varphi(x) + (0\backslash 0)) && 5.26\\
&= (0\backslash 0) \cdot \varphi(x) && 5.25\\
&= \varphi(\varphi(x)). && 5.24
\end{aligned}$$

This concludes the proof for the sufficiency of Theorem 5.5, and next we will show the necessity.

($\Leftarrow$) First note that since $(Q, +)$ is a commutative Moufang loop and $\psi\varphi^{-1}$ is a nuclear mapping, we have the following:

$$\begin{aligned}
(\psi\varphi^{-1}(a) + a) + (b + c) &= ((a + \psi\varphi^{-1}(a)) + (-a + a)) + (b + c)\\
&= ((a + (\psi\varphi^{-1}(a) + -a)) + a) + (b + c) && \text{CML}\\
&= ((a + (-a + \psi\varphi^{-1}(a))) + a) + (b + c)\\
&= (((-a + \psi\varphi^{-1}(a)) + a) + a) + (b + c)\\
&= ((-a + \psi\varphi^{-1}(a)) + (a + a)) + (b + c) && \psi\varphi^{-1} \text{ nuclear}\\
&= ((a + a) + (-a + \psi\varphi^{-1}(a))) + (b + c)\\
&= (a + a) + ((-a + \psi\varphi^{-1}(a)) + (b + c)) && \psi\varphi^{-1} \text{ nuclear}\\
&= (a + a) + (((-a + \psi\varphi^{-1}(a)) + b) + c) && \psi\varphi^{-1} \text{ nuclear}\\
&= a + (a + (((-a + \psi\varphi^{-1}(a)) + b) + c)) && \text{Moufang}
\end{aligned}$$

$$\begin{aligned}
&= a + ((((-a + \psi\varphi^{-1}(a)) + b) + c) + a) && \\
&= (a + ((-a + \psi\varphi^{-1}(a)) + b)) + (c + a) && \text{Moufang} \\
&= ((a + (-a + \psi\varphi^{-1}(a))) + b) + (c + a) && \psi\varphi^{-1} \text{ nuclear} \\
&= (\psi\varphi^{-1}(a) + b) + (c + a) && \text{Inverse property}
\end{aligned}$$

Thus, $\psi\varphi^{-1}$ satisfies (A1).

Now, using that $a \cdot b = (\psi(a) + \varphi(b)) + g$, φ and ψ are automorphisms of $(Q, +)$, $(Q, +)$ is a commutative Moufang loop, $\psi^2 = \varphi^2$, and $\psi\varphi^{-1}$ satisfies (A1) in $(Q, +)$, we have the following for every $a, b, c \in Q$:

$$\begin{aligned}
aa \cdot bc &= ((\psi(a) + \varphi(a)) + g) \cdot ((\psi(b) + \varphi(c)) + g) \\
&= (\psi((\psi(a) + \varphi(a)) + g) + \varphi((\psi(b) + \varphi(c)) + g)) + g \\
&= (((\psi^2(a) + \psi\varphi(a)) + \psi(g)) + ((\varphi\psi(b) + \varphi^2(c)) + \varphi(g))) + g
\end{aligned}$$

Since $\varphi, \psi \in$ Aut$(Q, +)$.

$$\begin{aligned}
&= (((\psi^2(a) + \psi\varphi(a)) + \psi\varphi^{-1}\varphi(g)) + ((\varphi\psi(b) + \varphi^2(c)) + \varphi(g))) + g \\
&= (((\psi^2(a) + \psi\varphi(a)) + (\varphi\psi(b) + \varphi^2(c))) + (\psi\varphi^{-1}\varphi(g) + \varphi(g))) + g
\end{aligned}$$

Since $(Q, +)$ is commutative and by (A1).

$$= (((\varphi^2(a) + \psi\varphi(a)) + (\varphi\psi(b) + \varphi^2(c))) + (\psi\varphi^{-1}\varphi(g) + \varphi(g))) + g$$

Since $\varphi^2 = \psi^2$.

$$\begin{aligned}
&= (((\varphi^2(a) + \psi\varphi^{-1}\varphi^2(a)) + (\varphi\psi(b) + \varphi^2(c))) + (\psi\varphi^{-1}\varphi(g) + \varphi(g))) + g \\
&= (((\varphi^2(c) + \psi\varphi^{-1}\varphi^2(a)) + (\varphi\psi(b) + \varphi^2(a))) + (\psi\varphi^{-1}\varphi(g) + \varphi(g))) + g
\end{aligned}$$

Since $(Q, +)$ is commutative and by (A1).

$$= (((\varphi^2(c) + \psi\varphi(a)) + \psi\varphi^{-1}\varphi(g)) + ((\varphi\psi(b) + \varphi^2(a)) + \varphi(g))) + g$$

Again, since $(Q, +)$ is commutative and by (A1).

$= (((\psi^2(c) + \psi\varphi(a)) + \psi(g)) + ((\varphi\psi(b) + \varphi^2(a)) + \varphi(g))) + g$

Since $\varphi^2 = \psi^2$.

$= (\psi((\psi(c) + \varphi(a)) + g) + \varphi((\psi(b) + \varphi(a)) + g)) + g$

Since $\varphi, \psi \in \text{Aut}(Q, +)$.

$= ((\psi(c) + \varphi(a)) + g) \cdot ((\psi(b) + \varphi(a)) + g)$

$= ca \cdot ba.$

Similarly, we can show $ab \cdot cc = cb \cdot ca$, thus $(Q, \cdot)$ is a semiparamedial quasigroup. □

Bibliography

[1] M. Aboras, *Dihedral-like constructions of automorphic loops*, Univ. of Denver, PhD Dissertation, (2015).

[2] C. Bergman, *Universal Algebra: Fundamentals and Selected Topics*, Chapman & Hall, CRC Press, (2011).

[3] V.D. Belousov, The structure of distributive quasigroups, *Mat. Sb. (N.S.)* **50**(92):3 (1960), 267–298.

[4] V.D. Belousov, Balanced identities in quasigroups (in Russian), *Mat. Sbornik* (N.S.), **70** (1966), 55–97.

[5] R.H. Bruck, Some results in the theory of quasigroups, *Trans. Amer. Math. Soc.* **55** (1944), 19–52.

[6] R.H. Bruck, *Survey of Binary Systems*, Springer Verlag, (1971).

[7] R.H. Bruck, L.J. Paige, Loops whose inner mappings are automorphisms, *Ann. of Math.* (2) **63** (1956), 308–323.

[8] S. Burris, H.P. Sankappanavar, *A Course in Universal Algebra*, Grad. Texts in Math., **78**, Springer-Verlag, New York, Berlin, (1981).

[9] K. Conrad, *Generalized Quaternions*, https://kconrad.math.uconn.edu/blurbs/grouptheory/genquat.pdf, Accessed 29 April, 2022.

[10] O. Chein, M.K. Kinyon, A. Rajah, P. Vojtěchovský, Loops and the Lagrange property, *Results Math.* **43** (2003), no. 1-2, 74–78.

[11] A. Drápal, On multiplication groups of relatively free quasigroups isotopic to abelian groups, *Czechoslovak Math. J.* **55** (2005), 61–86.

[12] D. Dummit, R. Foote, *Abstract Algebra*, 3rd ed., John Wiley and Sons, Inc., Hoboken, (2004).

[13] E. Falconer, Isotopy invariants in quasigroups, *Trans. Amer. Math. Soc.* **151** (1970), 511–526.

[14] I.A. Florja, Bol quasigroups (in Russian), *Studies in General Algebra*, Ştiinţa, Chişinău, (1965), 136–154.

[15] R. Freese, R. McKenzie, *Commutator Theory for Congruence Modular Varieties*, London Math. Soc. Lecture Note Ser., **125**, Cambridge University Press, Cambridge, (1987).

[16] The Gap Group: GAP – groups algorithms, and programming, Version 4.11.1. https://www.gap-system.org/ (2021), Accessed 29 April, 2022.

[17] A. Grishkov, M.K. Kinyon, G.P. Nagy, Solvability of commutative automorphic loops *Proc. Amer. Math. Soc.* **142** (2014), 3029–3037.

[18] G. Janelidze, M.C. Pedicchio, Pseudogroupoids and commutators, *Theory and Applications of Categories*, **8** (2001), 408–456.

[19] P. Jedlička, M.K. Kinyon, P. Vojtěchovský, The structure of commutative automorphic loops, *Trans. of Am. Math. Soc.* **363**(1) (2011), 365–384.

[20] P. Jedlička, D. Stanovský and P. Vojtěchovský, Distributive and trimedial quasigroups of order 243, *Discrete Math.* **340** (2017), 404–415.

[21] J. Ježek, T. Kepka, Quasigroups, isotopic to a group, *Comment. Math. Univ. Carolin.* **16**(1) (1975), 59–76.

[22] K.W. Johnson, M.K. Kinyon, G.P. Nagy, P. Vojtěchovský, Searching for small simple automorphic loops, *LMS J. Comput. Math.* **14** (2011), 200-213.

[23] T. Kepka, Structure of triabelian quasigroups, *Comment. Math. Univ. Carolin.* **17**(2) (1976), 229–240.

[24] T. Kepka, F-quasigroups isotopic to Moufang loops, *Czechoslovak Math. J.* **29** (1979), 62–83.

[25] T. Kepka, A note on WA-quasigroups, *Acta Univ. Carolin. Math. Phys.* **19**(2) (1978), 61–62.

[26] T. Kepka, M. Kinyon and J.D. Phillips, The structure of F-quasigroups, *J. Algebra* **317** (2007), 435–461.

[27] T. Kepka, P. Němec, T-quasigroups, I , *Acta Univ. Carolin. Math. Phys.* **12** (1971), 39–49.

[28] M.K. Kinyon, K. Kunen, J.D. Phillips, P. Vojtěchovský, The structure of automorphic loops, *Trans. of Am. Math. Soc.* **368**(12) (2016), 8901–8927.

[29] W. McCune, "Prover9 and Mace4", http://www.cs.unm.edu/˜mccune/Prover9, (2005-2010). Accessed 29 April, 2022.

[30] R. McKenzie, J. Snow, Congruence modular varieties: commutator theory and its uses, *Structural theory of automata, semigroups, and universal algebra,* NATO Science Series II: Math. Phy. and Chem. Series, **207**, Springer, Dordrecht, (2005), 273–329.

[31] D.C. Murdoch, Structure of abelian quasigroups, *Trans. Amer. Math. Soc.* **49** (1941), 392–409.

[32] G. Nagy, P. Vojtěchovský, "RightQuasigroups": computing with loops and quasigroups in GAP. Provided by authors upon request.

[33] H.O. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma Ser. Pure Math. **8**, Heldermann-Verlag, (1990).

[34] D. Robinson, Bol quasigroups, *Publ. Math. Debrecen 19* (1972), 151–153.

[35] W.R. Scott, *Group Theory*, Dover Publications, (1987).

[36] V. Shcherbacov, *Elements of quasigroup theory and applications*, Monographs and Research Notes in Mathematics. CRC Press, (2017).

[37] J.D.H. Smith, *Mal'cev Varieties*, Lecture Notes in Math., **554**, Springer-Verlag, Berlin, (1976).

[38] J.D.H. Smith, *An Introduction to Quasigroups and their Representations*, Studies in Advanced Mathematics. Chapman & Hall/CRC, (2007).

[39] J.-P. Soublin, Etude algébrique de la notion de moyenne (French). *J. Math. Pures Appl.* **50** (1971), 53–264.

[40] D. Stanovský and P. Vojtěchovský, Commutator theory for loops, *J. Algebra*, **399** (2014), 290–322.

[41] D. Stanovský and P. Vojtěchovský, Abelian extensions and solvable loops, *Results. Math.*, **66** (2014), 367–384.

[42] K. Toyoda, On axioms of linear functions, *Proc. Imp. Acad. Tokyo* **17** (1941), 221–227.

Appendix A. GAP Code

The following is the GAP code used to construct quaternionic automorphic loops. The function takes as its input a number n such that $n = 2^k$ and an automorphism a of $\mathbb{Z}_{2^{k-1}}$, where a is an invertible element of the ring with order 2. As discussed in Chapter 4, there are only three for any given 2^k: -1, $2^{k-2}-1$, and $2^{k-2}+1$. Then the code returns the quaternionic automorphic loop of order $n = 2^k$ constructed on $\mathbb{Z}_{2^{k-1}} \times \mathbb{Z}_4$ with multiplication given by $(i,u)(j,v) = (a^{uv}(i + (-1)^u v), v + v)$. This code requires the RightQuasigroups package developed by Gábor P. Nagy and Petr Vojtěchovský [32].

```
QuaternionAutomorphicLoop := function( n, a )
  local m, el, ct, r, s, i, j, u, v, k, w, q;
    if IsOddInt(n) or not IsPrimePowerInt(n) then
      Error("The order must be a power of 2.");
    fi;
    m:=n/2;
    el := Cartesian([0..(m-1)], [0..3]); \# |q|=4m=2n
    ct := List([1..2*n],r-> List([1..2*n],s-> []));
    for r in [1..2*n] do
      for s in [1..2*n] do
        i:=el[r][1]; j:=el[s][1];
        u:=el[r][2]; v:=el[s][2];
        k := ((i + (-1)\^{}u * j)*(a\^{}(u*v))) mod m;
        w := (u + v) mod 4;
        ct[r][s] := [k,w];
      od;
    od;
  q := LoopByCayleyTable(ct);
  return FactorLoop(q,Subloop(q,[[m/2,2]]));
end;
```