Loops and Their Permutation Groups

Mark Greer
University of Denver

Follow this and additional works at: https://digitalcommons.du.edu/etd

Part of the Mathematics Commons

Recommended Citation
Greer, Mark, "Loops and Their Permutation Groups" (2013). Electronic Theses and Dissertations. 246.
https://digitalcommons.du.edu/etd/246

This Dissertation is brought to you for free and open access by the Graduate Studies at Digital Commons @ DU. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of Digital Commons @ DU. For more information, please contact jennifer.cox@du.edu,dig-commons@du.edu.
Loops and their Permutation Groups

A Dissertation
Presented to the Faculty
of Natural Sciences and Mathematics
University of Denver

in Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

by
Mark Greer
June 2013
Advisor: Michael Kinyon
Abstract

This dissertation uses the connections between loops and their associated permutation groups to study certain varieties of loops. We first define a variety of loops generalizing commutative automorphic loops and show this new variety is power associative. We show a correspondence to Bruck loops of odd order and use this correspondence to give structural results for our new variety, which in turn hold for commutative automorphic loops. Next, we study a variety of loops that generalize both Moufang and Steiner loops. We extend on known results for Moufang loops and then extend two different doubling constructions for creating Moufang and other varieties of loops. We then give a general construction to create simple RCC loops from $GL(2, q)$ for $q$ a prime power. Finally, we consider a generalization of Bruck loops, and show that different companions of pseudoautomorphism live in certain subloops.
Acknowledgements

I have many people thank and this in no way represents a complete list of everyone who has supported me on this journey. I want to first and foremost thank Jeff Rushall and Dr. Roy St. Laurent, both at Northern Arizona University. Without your support and guidance during a difficult period in my life, none of this would be possible. I am forever grateful for all your advice and help.

I would like to thank all the wonderful people in the Math department at the University of Denver, especially Liane Beights and Don Oppliger. Both of you helped me many times with different problems, most of which I created! I would also like to thank the wonderful faculty and graduate students that I have had the pleasure of meeting and working with over my time at DU. I would like to thank specifically Nikolaos Galatos and Larry Berliner for reading this dissertation and serving on my PhD committee.

I am forever indebted to my advisor Michael Kinyon, not only for introducing me to the field, but for all the time helping me along the way. I can in no way ever repay you for the countless hours you spent with me on my own research, mathematics and life in general. In the same vain, I would like to thank Petr Vojtěchovský for all the useful comments and discussions about loop theory and general mathematics.

Finally, I would like to thank all my family and friends for the support throughout this past several years, especially my wife Victoria. Without your love, patience and support, none of this would be possible. I am completely certain that I would not be at this point in my life without you by my side.
# Table of Contents

Acknowledgements .......................................................... iii
List of Tables ................................................................. vi

1 Introduction .......................................................................... 1
   1.1 Preliminaries .............................................................. 2
   1.2 Special Varieties of loops .............................................. 9
   1.3 Summary of Results ................................................... 12

2 $\Gamma$-Loops ....................................................................... 14
   2.1 $\Gamma$-loops ............................................................... 15
   2.2 $\Gamma$-Loops are power-associative ................................. 20
   2.3 Twisted subgroups and uniquely 2-divisible Bruck loops ... 23
   2.4 Inverse functors .......................................................... 29
   2.5 $\Gamma$-loops of odd order .............................................. 32
   2.6 Constructing commutative automorphic loops ................. 36

3 Semiautomorphic Inverse Property Loops ......................... 40
   3.1 Semiautomorphic inverse property loops ....................... 40
   3.2 Commutant of a Semiautomorphic loop ......................... 44
   3.3 Constructing semiautomorphic IP loops ......................... 52
      3.3.1 Generalizing Chein’s Construction ......................... 53
      3.3.2 Generalizing de Barros-Juriaans’ Construction ........ 61
   3.4 Connections between the extended Chein and extended de Barros- Juriaans constructions ........................................ 67
   3.5 Conclusion .................................................................. 75

4 Simple Right Conjugacy Closed Loops ............................ 90
   4.1 Right Conjugacy Closed loops .................................... 91
   4.2 Constructing Simple RCC loops .................................. 92
   4.3 Conclusion ................................................................ 100
5 Pseudoautomorphisms of Bruck loops and their generalizations 105
  5.1 Weak commutative inverse property loops . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 106

Bibliography 111

Appendix A 115
List of Tables

2.1 The smallest Γ-loop ................................................. 20
3.1 Multiplication Table for \((Q_2, \circ_2)\) .............................. 69
3.2 Multiplication Table for \((Q_1, \circ_1)\) .............................. 72
3.3 Multiplication Table for \((Q_2, \circ_2)\) .............................. 72
3.4 A non-semiautomorphic flexible C-loop ........................... 89
4.1 Multiplication Table for \((Q, \circ_f)\) ................................. 102
4.2 Table of RCC Loops .................................................. 104
Chapter 1

Introduction

Loop theory studies algebraic structures generalizing groups. Informally, loops are “nonassociative groups,” that is, they have identity elements \(1x = x1 = x\), and equations \(ax = b\), \(ya = b\) can be uniquely solved, but the structure need not be associative. Loops (and quasigroups) are not just generalizations for the sake of generalization. They appear quite naturally in many parts of mathematics. Historically, loop theory is most closely connected with combinatorics, particularly latin squares. Indeed, normalized latin squares are precisely the multiplication tables of finite loops. Loops are also the coordinatizing structures for 3-nets, which are close relatives of projective planes.

Just as in group theory, in a loop one considers the left and right translation maps \(y \mapsto xy\) and \(y \mapsto yx\). Thus, for a given loop, we can associate several permutation groups generated by these maps. It is therefore easy to see why deep problems in loop theory often lead to deep and interesting problems in group theory and other areas of mathematics. This dissertation focuses on the connections between several varieties of loops and their associated permutation groups.
1.1 Preliminaries

In this section, we introduce basic notions of quasigroup and loop theory. Standard references for both are [8, 42].

Let \( Q \) be a set and \( \cdot \) a binary operation on \( Q \). Then \( (Q, \cdot) \) is a \textit{magma}. A magma is a \textit{quasigroup} if for any \( a, b \in Q \) there exists a unique \( x, y \in Q \) such that \( a \cdot x = b \) and \( y \cdot a = b \). We define the \textit{left translation by} \( a \) \textit{in} \( Q \) as the mapping \( L_a : Q \rightarrow Q \) given by

\[
xL_a = ax.
\]

Similarly, we define the \textit{right translation by} \( a \) \textit{in} \( Q \) as the mapping \( R_a : Q \rightarrow Q \) given by

\[
xR_a = xa.
\]

It is clear that \( (Q, \cdot) \) is a quasigroup \textit{if and only if} \( L_a \) and \( R_a \) are bijections for all \( a \in Q \). In the finite case, the multiplication table for a finite quasigroup is precisely a latin square. Since \( L_a \) and \( R_a \) are bijections, the inverse mappings exist and we can define \( L_a^{-1} \) and \( R_a^{-1} \). Defining \( /, \backslash \) as

\[
xL_a^{-1} = a \backslash x \quad xR_a^{-1} = x / a,
\]

we see that

\[
a \backslash (a \cdot x) = xL_aL_a^{-1} = b = a \cdot (a \backslash x) = xL_a^{-1}L_a,
\]

\[
(x \cdot a) / a = xR_aR_a^{-1} = b = (x / a) \cdot a = xR_a^{-1}R_a.
\]

Thus, a quasigroup can be seen as a universal algebra \( (Q, \cdot, /, \backslash) \). Each of the three definitions is equivalent, however the last ensures that quasigroups are closed under
homomorphic images, and hence a variety. We will use either of the three equivalent definitions interchangeably.

A quasigroup \( Q \) is a loop if \( Q \) contains a neutral element \( 1 \in Q \) such that

\[
1 \cdot x = x = x \cdot 1.
\]

holds for all \( x \in Q \). It is clear that if \( Q \) has a neutral element, it is unique. In the finite case, the multiplication table of a finite loop is precisely a normalized latin square.

Quasigroups, and hence loops, need not be associative. In fact, associative loops are exactly groups. To avoid excessive parentheses, we use the following convention:

- multiplication \( \cdot \) will be less binding than divisions \( \div \),
- divisions are less binding than juxtaposition.

For example \( xy/z \cdot y \div xy \) reads as \( ((xy)/z)(y \div (xy)) \).

We define the left section of \( Q \) and right section of \( Q \) as \( L_Q = \{ L_x \mid x \in Q \} \) and \( R_Q = \{ R_x \mid x \in Q \} \) respectively. We then have the left multiplication group of \( Q \), \( \text{Mlt}_\lambda(Q) = \langle L_Q \rangle \) and right multiplication group of \( Q \), \( \text{Mlt}_\rho(Q) = \langle R_Q \rangle \) and the multiplication group of \( Q \), \( \text{Mlt}(Q) = \langle \text{Mlt}_\lambda(Q), \text{Mlt}_\rho(Q) \rangle \). We also define the right inner mapping group of \( Q \) \( \text{Inn}_\rho(Q) = \{ \theta \in \text{Mlt}_\rho(Q) \mid 1\theta = 1 \} \), the left inner mapping group of \( Q \) \( \text{Inn}_\lambda(Q) = \{ \theta \in \text{Mlt}_\lambda(Q) \mid 1\theta = 1 \} \) and the inner mapping group of \( Q \), \( \text{Mlt}(Q)_1 = \text{Inn}(Q) = \{ \theta \in \text{Mlt}(Q) \mid 1\theta = 1 \} \).

The following proposition uses right translations to check whether a magma \((Q, \cdot)\) is a loop or not.
Proposition 1.1.1. ([28]) Let \((Q, \cdot)\) be a magma with \(1 \in Q\) an identity element. Then \(Q\) is a loop if and only if \(R_xR_y^{-1}\) is fixed point free for every \(x, y \in Q\) with \(x \neq y\) and \(x, y \neq 1\).

Proof. This follows from Lemmas 2.1 and 2.2. \(\square\)

Consider the following special mappings:

\[
T_x = R_xL_x^{-1}, \quad R_{x,y} = R_xR_yR_{xy}^{-1}, \quad L_{x,y} = L_xL_yL_{yx}^{-1}.
\]

Note that \(T_x\) is conjugation, measuring the lack of commutativity, and \(L_{x,y}, R_{x,y}\) measure the lack of associativity. Hence, \(L_{x,y}, R_{x,y}\) are trivial precisely when \(Q\) is a group.

Lemma 1.1.2 ([8]). \(\text{Inn}(Q) = \langle T_x, L_{x,y}, R_{x,y} \mid \forall x, y \in Q \rangle\). 

For a loop \(Q\), a subset \(S\) of \(Q\) is a subloop if \((S, \cdot, \setminus, /)\) is a loop. A subloop \(N\) of a loop \(Q\) is a normal subloop, \(N \trianglelefteq Q\), if it is invariant under \(\text{Inn}(Q)\). Moreover, using Lemma 1.1.2, we have that a subloop \(N\) is normal if and only if 

\[
xN = Nx \quad x(yN) = (xy)N \quad (Nx)y = N(xy)
\]

holds for all \(x, y \in Q\).

In a loop \(Q\) with identity 1, for all \(x \in Q\) there exists a unique left inverse \(x^\lambda\) and unique right inverse \(x^\rho\) such that \(x^\lambda x = xx^\rho = 1\). Note \(x^\lambda = x^\rho\) exactly when \(x\) has a unique two-sided inverse denoted by \(x^{-1}\). When \(Q\) has two-sided inverses for all \(x, y \in Q\), we can define the left inverse property, (LIP), \(x^{-1}(xy) = y ⇔ L_{x^{-1}} = L_x^{-1}\) and the right inverse property, (RIP), \((yx)x^{-1} = y ⇔ R_{x^{-1}} = R_x^{-1}\). A loop \(Q\) has the
inverse property, (IP), if $Q$ has both the (LIP) and (RIP). Similarly, we define the antiautomorphic inverse property, (AAIP), $(xy)^{-1} = y^{-1}x^{-1}$ and the automorphic inverse property, (AIP), $(xy)^{-1} = x^{-1}y^{-1}$. Note that an IP loop satisfies (AAIP).

Finally we define the weak commutative inverse property, (WCIP), $(xy)^{-1} = y^{-1}x^{-1}$. In a loop with two-sided inverses, let $J : Q \to Q$ be the mapping defined by $xJ = x^{-1}$. Then (AAIP) is equivalent to $LxJ = JRx$, (AIP) is equivalent to $LxJ = JLx$, and (WCIP) is equivalent to $RxJR = J$.

In a loop $Q$, we define the left alternative property, (LAP) as $x(xy) = x^2y$. Similarly, we have the right alternative property, (RAP), $(yx)x = yx^2$. A loop $Q$ is said to be alternative if $Q$ satisfies both (LAP) and (RAP) for all $x, y \in Q$. We also define the flexible law, (FLEX), as $x(yx) = (xy)x$ and a loop is called flexible if it satisfies (FLEX) for all $x, y \in Q$.

In a loop $Q$, we set $x^n = 1L^n_x$ for all $x \in Q$ and for all $n \in \mathbb{Z}$. A loop $Q$ is power-associative if every 1-generated subloop is a group. That is, $\langle x \rangle$ is a subgroup for all $x \in Q$. This is easily seen to be equivalent to $x^m x^n = x^{m+n}$ for every $x \in Q$ and for all $m, n \in \mathbb{Z}$. Similarly, $Q$ is diassociative if $\langle x, y \rangle$ is a subgroup for all $x, y \in Q$.

For a loop $Q$, we have the following subsets:

- the left nucleus of $Q$, $N_\lambda(Q) = \{ a \in Q \mid a \cdot xy = ax \cdot y \ \forall x, y \in Q \}$,
- the middle nucleus of $Q$, $N_\mu(Q) = \{ a \in Q \mid x \cdot ay = xa \cdot y \ \forall x, y \in Q \}$,
- the right nucleus of $Q$, $N_\rho(Q) = \{ a \in Q \mid x \cdot ya = xy \cdot a \ \forall x, y \in Q \}$,
- the nucleus of $Q$, $N(Q) = N_\lambda(Q) \cap N_\mu(Q) \cap N_\rho(Q)$,
- the commutant of $Q$, $C(Q) = \{ a \in Q \mid xa = ax \ \forall x \in Q \}$,
- the center of $Q$, $Z(Q) = N(Q) \cap C(Q)$.

For a loop $Q$, the nuclei $N(Q), N_\lambda(Q), N_\mu(Q), N_\rho(Q)$, and $N(Q)$ are all subloops of $Q$ and the center $Z(Q)$ is a normal subloop of $Q$. However, the commutant, $C(Q)$ need not
be a subloop in general of $Q$.

**Proposition 1.1.3.** Let $Q$ be a loop. Then $a \in C(Q) \cap N_\lambda(Q) \iff R_a \in Z(\text{Mlt}_\rho(Q))$.

**Proof.** Let $a \in C(Q) \cap N_\lambda(Q)$. Then $\forall x, y \in Q$,

$$yR_aR_x = ya \cdot x = ay \cdot x = a \cdot yx = yx \cdot a = R_yR_aR_x.$$

Hence, $R_a \in Z(\text{Mlt}_\rho(Q))$. Conversely, let $R_a \in Z(\text{Mlt}_\rho(Q))$. Then $ax = 1R_aR_x = 1R_xR_a = xa$. Hence $a \in C(Q)$. Moreover,

$$a \cdot yx = yx \cdot a = yR_xR_a = yR_aR_x = a \cdot x = ay \cdot x.$$

Thus, $a \in C(Q) \cap N_\lambda(Q)$. \hfill \Box

A bijection $\theta : Q \to Q$ is an automorphism if $(xy)\theta = x\theta \cdot y\theta$ for all $x, y \in Q$. We therefore have the automorphism group of $Q$, $\text{Aut}(Q) = \{ \theta : Q \to Q \mid \theta \text{ is an automorphism of } Q \}$. A triple $(\alpha, \beta, \gamma)$ of permutations of a loop $Q$ is an autotopism if for all $x, y \in Q$, $x\alpha \cdot y\beta = (xy)\gamma$. The set $\text{Atp}(Q)$ of all autotopisms of $Q$ is a group under composition. Of particular interest here are the three subgroups

$$\text{Atp}_\lambda(Q) = \{ (\alpha, \beta, \gamma) \in \text{Atp}(Q) \mid 1\beta = 1 \},$$

$$\text{Atp}_\mu(Q) = \{ (\alpha, \beta, \gamma) \in \text{Atp}(Q) \mid 1\gamma = 1 \},$$

$$\text{Atp}_\rho(Q) = \{ (\alpha, \beta, \gamma) \in \text{Atp}(Q) \mid 1\alpha = 1 \}.$$

For instance, say, $(\alpha, \beta, \gamma) \in \text{Atp}_\lambda(Q)$. For all $x \in Q$, $x\alpha = x\alpha \cdot 1 = x\alpha \cdot 1\beta = (x1)\gamma = x\gamma$. Thus $\alpha = \gamma$. Set $a = 1\alpha$. For all $x \in Q$, $x\alpha = (1x)\alpha = 1\alpha \cdot x\beta = a \cdot x\beta$

Thus $\alpha = \beta L_a$, and so every element of $\text{Atp}_\lambda(Q)$ has the form $(\beta L_a, \beta, \beta L_a)$ for
some $a \in Q$. Conversely, it is easy to see that if a triple of permutations of that form is an autotopism, then $1\beta = 1$.

By similar arguments for the other two cases, we have the following characterizations:

\[ \text{Atp}_L(Q) = \text{Atp}(Q) \cap \{ (\beta L_a, \beta, \beta L_a) \mid \beta \in \text{Sym}(Q), a \in Q \}, \]
\[ \text{Atp}_\mu(Q) = \text{Atp}(Q) \cap \{ (\gamma R^{-1}_c, \gamma L^{-1}_c, \gamma) \mid \gamma \in \text{Sym}(Q), c \in Q \}, \]
\[ \text{Atp}_\rho(Q) = \text{Atp}(Q) \cap \{ (\alpha, \alpha R_b, \alpha R_b) \mid \alpha \in \text{Sym}(Q), b \in Q \}. \]

Since these special types of autotopisms are entirely determined by a single permutation and an element of the loop, it is customary to focus on those instead of on the autotopisms themselves. This motivates the following definitions.

Let $Q$ be a loop. If $\beta \in \text{Sym}(Q)$ and $a \in Q$ satisfy

\[ a \cdot (xy)\beta = (a \cdot x\beta)(y\beta) \quad (1.1.1) \]

for all $x, y \in Q$, then $\beta$ is called a left pseudoautomorphism with companion $a$. If $\gamma \in \text{Sym}(Q)$ and $c \in Q$ satisfy

\[ (xy)\gamma = [(x\gamma)/(c \setminus 1)][c \setminus (y\gamma)] \quad (1.1.2) \]

for all $x, y \in Q$, then $\gamma$ is called a middle pseudoautomorphism with companion $c$. Finally, if $\alpha \in \text{Sym}(Q)$ and $b \in Q$ satisfy

\[ (xy)\alpha \cdot b = (x\alpha)(y\alpha \cdot b) \quad (1.1.3) \]
for all \( x, y \in Q \), then \( \alpha \) is called a right pseudoautomorphism with companion \( b \).

We denote the identity mapping on \( Q \) by \( \iota \).

**Lemma 1.1.4.** Let \( Q \) be a loop. The nuclei are characterized as follows:

\[
N_\lambda(Q) = \{a \in Q \mid (tLa, t, tLa) \in \text{Atp}(Q)\}
\]

\[
= \{a \in Q \mid \iota \text{ is a left pseudoautomorphism with companion } a\},
\]

\[
N_\mu(Q) = \{c \in Q \mid (t Rc, tLc^{-1}, t) \in \text{Atp}(Q)\}
\]

\[
= \{c \in Q \mid \iota \text{ is a middle pseudoautomorphism with companion } c\},
\]

\[
N_\rho(Q) = \{b \in Q \mid (t, tRb, tRb) \in \text{Atp}(Q)\}
\]

\[
= \{b \in Q \mid \iota \text{ is a right pseudoautomorphism with companion } b\}.
\]

**Proof.** Perhaps the only claim which is not immediately obvious is the characterization of the middle nucleus. Suppose \( \iota \) is a middle pseudoautomorphism with companion \( c \). Then for all \( x, y \in Q \), \( xy = [x/(c\1)][c\ y] \). Replace \( y \) with \( cy \) to get \( x \cdot cy = [x/(c\1)]y \). Set \( y = 1 \) so that \( xc = x/(c\1) \). Thus \( x \cdot cy = xc \cdot y \), that is, \( c \in N_\mu(Q) \). The reverse inclusion is similarly straightforward. \( \square \)

Observe that a permutation \( \sigma \) is an automorphism if and only if it is a pseudoautomorphism of any of the three types with companion 1. The following is also clear from Lemma 1.1.4.

**Lemma 1.1.5.** Let \( Q \) be a loop. If \( \sigma \in \text{Sym}(Q) \) is a left [middle, right] pseudoautomorphism with companion \( c \in Q \) then \( \sigma \) is an automorphism if and only if \( c \in N_\lambda(Q) [N_\mu(Q), N_\rho(Q)] \).

Finally, for a flexible loop \( Q \), the mapping \( \theta : Q \to Q \) is a semiautomorphism of \( Q \) if (i) \( 1 \theta = 1 \) and (ii) \( (xy)\theta = x\theta y\theta x\theta \). Note that every automorphism is a
semiautomorphism and in a flexible loop with (AAIP), inversion is a semiautomorphism.

1.2 Special Varieties of loops.

A loop $Q$ is a Moufang loop if any of the following equivalent identities hold for all $x, y, z \in Q$

$$xy \cdot zx = x(yz \cdot x), \quad x(y \cdot xz) = (xy \cdot x)z, \quad x(y \cdot xz) = (x \cdot yz)y.$$  

Moufang loops are easily the most studied variety of loops. The first main structural result for Moufang loops is Moufang’s Theorem, proved originally by Moufang [38]. We say that $x, y, z$ associate if $xy \cdot z = x \cdot yz$.

**Theorem 1.2.1. (Moufang’s Theorem)** Let $Q$ be a Moufang loop with $x, y, z \in Q$, not necessarily distinct. Then $\langle x, y, z \rangle$ is a subgroup if and only if $x, y, z$ associate.

This immediately proves Moufang loops are power associative. Moreover, Moufang loops are diassociative (since the Moufang identities immediately imply (LAP), (RAP), and (FLEX) and hence are inverse property, alternative, flexible loops).

Many natural examples of Moufang loops are known. One example is typified by the sphere $S^7$ under octonion multiplication, or more generally, the set of all nonzero octonions under multiplication. Even more generally, one can take the set of all invertible elements in an alternative ring. Moufang loops are closely related to groups with triality (and in fact, these notions are essentially the same [12]). The deepest questions in the theory of Moufang loops are often resolved by formulating
them in group theoretic terms and using the corresponding powerful tools of group theory. For instance, all finite simple Moufang loops are classified because finite simple groups with triality are classified [36].

A loop $Q$ is said to be a (left) Bruck loop if it satisfies the (left) Bol identity $[x(yx)]z = x[y(xz)]$ for all $x, y, z \in Q$ and the (AIP). Bruck loops have also been called “K-loops” [30] or “gyrocommutative gyrogroups” [47]. Dually, we define a (right) Bruck loop. In a Bruck loop $Q$, inverses are two-sided, and moreover, in a (left) Bruck loop, the (LIP) holds. Dually, in a (right) Bruck loop, (RIP) holds. Bruck loops have been intensively studied in recent years [1, 2, 4, 6, 5, 17, 30, 39].

The interest in Bruck loops is partly because they are a naturally occurring class. The set $\{v \in \mathbb{R}^3 \mid |v| < c\}$ of all relativistic velocity vectors forms a loop where the operation is Einstein’s velocity addition formula. This is an example of a Bruck loop [47]. Another example of a Bruck loop is given on the set $H^+(n, \mathbb{C})$ of all $n \times n$ positive definite Hermitian matrices by the polar decomposition. Given two such matrices $A$ and $B$, let $AB = PU$ be the polar decomposition where $P$ is positive definite Hermitian and $U$ is unitary. Defining $A \circ B = P$ gives $H^+(n, \mathbb{C})$ the structure of a Bruck loop [30].

A loop $Q$ is an automorphic loop if every inner mapping of $Q$ is an automorphism of $Q$ (i.e. $\text{Inn}(Q) \leq \text{Aut}(Q)$). From Lemma 1.1.2, we have

**Proposition 1.2.2** ([9]). A loop $Q$ is automorphic if and only if for all $x, y, u, v \in Q$;

\[
(uy)R_{x,y} = uR_{x,y} \cdot vR_{x,y},
\]

\[
(uy)L_{x,y} = uL_{x,y} \cdot vL_{x,y},
\]

\[
(uy)T_x = uT_x \cdot vT_x.
\]
Hence, the class of automorphic loops form a variety. Note that the variety of automorphic loops contains groups and commutative Moufang loops [8]. Automorphic loops were first studied by Bruck and Paige [9]. Recently, automorphic loops were shown to satisfy the Odd Order Theorem [33]. For automorphic loops of odd order, the Cauchy Theorem is known [33]. Also, automorphic loops satisfy the elementwise Lagrange Theorem (i.e. the order of an element divides the order of the loop) [33]. Finally, it has been shown in commutative automorphic loops that the Odd Order, Lagrange and Cauchy Theorems, as well as the nontriviality of the center of finite commutative automorphic $p$-loops ($p$ odd) all hold [26, 25, 27].

We say a subset $S$ of a group $G$ is closed under conjugation if $x^{-1}yx \in S$ for all $x, y \in S$. A loop $Q$ is a right conjugacy closed loop (or RCC loop) if $R_Q$ is closed under conjugation. That is, $R_x^{-1}R_yR_x \in R_Q$ for all $x, y \in Q$. Much of the literature deals with two-sided conjugacy closed loops (CC loops) which are RCC loops that are also left conjugacy closed (LCC), that is, $L_x^{-1}L_yL_x \in L_Q$ for all $x, y \in Q$.

A loop $Q$ is a Steiner loop if for all $x, y \in Q$

$$xy = yx \quad x(yx) = y.$$  

Note that this implies $xx = 1$ for all $x \in Q$, and hence Steiner loops have exponent 2. Steiner loops arise in combinatorics, since they correspond to Steiner triple systems.
1.3 Summary of Results

The dissertation is organized as follows. Commutative automorphic loops and Bruck loops have a deep connection in the odd order case, that is, one can construct a Bruck loop from a commutative automorphic loop of odd order using the left multiplication group. In Chapter 2 we define a new variety of loops, Γ-loops (§2.1) which generalize commutative automorphic loops. Our first major result is that Γ-loops are power-associative (§2.2). We then go on to construct Bruck loops from uniquely 2-divisible Γ-loops and construct Γ-loops from Bruck loops of odd order (§2.3) using the left multiplication group as before. Our main goal is showing a categorical isomorphism between (left) Bruck loops of odd order and Γ-loops of odd order (§2.4). Once this has been established, we can use the well known structure of Bruck loops of odd order to derive the Odd Order, Lagrange and Cauchy Theorems for Γ-loops of odd order, as well as the nontriviality of the center of finite Γ-p-loops (p odd) (§2.5). This answer in the affirmative a question posed by Jedlička, Kinyon and Vojtěchovský about the existence of Hall π-subloops and Sylow p-subloops in commutative automorphic loops. Finally we give a general construction for creating commutative automorphic loops (§2.6).

Both Moufang and Steiner loops are IP loops in which every inner mapping is a semiautomorphism. Hence, in Chapter 3, we study a variety of IP loops with this property as their defining axiom, called semiautomorphic, inverse property loops. Our first result shows an equivalence to a previously defined variety of loops (§3.1). Since semiautomorphic, inverse property loops generalize Moufang and Steiner loops, we extend several known results for Moufang and Steiner loops. In particular, the commutant is a subloop and if a is in the commutant, then $a^2$ is a
Moufang element, $a^3$ is a $C$-element and $a^6$ is in the center (§3.2). We then give two constructions for semiautomorphic inverse property loops based on Chein’s and de Barros and Juriaans’ doubling constructions (§3.3). In (§3.4) we consider what happens when we use the previous constructions multiple times. Finally we end by considering these new constructions on other diassociative loops (§3.5).

In *Chapter 4* we give constructions for creating simple RCC loops using the general linear group $GL(2,q)$ for $q$ a prime power. Simple RCC loops are known to exist, however, it is unclear for which orders there exist simple RCC loops. Using this construction, we can create simple RCC loops of order $q^2 - 1$ and $\frac{q^2-1}{2}$.

In *Chapter 5* we show that in a weak commutative inverse property loop, such as a (right) Bruck loop, if $\alpha$ is a right [left] pseudoautomorphism with companion $c$, then $c \cdot c^2$ must lie in the left nucleus. In particular, for any such loop with trivial left nucleus, every right pseudoautomorphism is an automorphism and if the squaring map is a permutation, then every left pseudoautomorphism is an automorphism as well. We also show that every pseudoautomorphism of a commutative inverse property loop is an automorphism, generalizing a well-known result of Bruck.

Throughout this dissertation, we often use the GAP system [22], more specifically the LOOPS package [40], for constructing and analyzing various examples. We also use the automated deduction program PROVER9 and the finite model builder MACE4, both developed by McCune [37]. Many of the results presented in this dissertation can also be found in [20, 19, 21].
Chapter 2

Γ-Loops

Let $G$ be a uniquely 2-divisible group, that is, a group in which the map $x \mapsto x^2$ is a bijection. On $G$ we define two new binary operations as follows:

\begin{align*}
  x \oplus y &= (xy^2x)^{1/2}, \quad (2.0.1) \\
  x \odot y &= xy[y,x]^{1/2}. \quad (2.0.2)
\end{align*}

Here $a^{1/2}$ denotes the unique $b \in G$ satisfying $b^2 = a$ and $[y,x] = y^{-1}x^{-1}yx$. Then it turns out that both $(G, \oplus)$ and $(G, \odot)$ are loops with neutral element 1. Both loops are power-associative, which informally means that integer powers of elements can be defined unambiguously. Further, powers in $G$, powers in $(G, \oplus)$ and powers in $(G, \odot)$ all coincide.

For $(G, \oplus)$ all of this is well-known with the basic ideas dating back to Bruck [8] and Glauberman [17]. $(G, \oplus)$ is an example of a Bruck loop. Jedlička, Kinyon and Vojtěchovský [26] showed that starting with a uniquely 2-divisible commutative automorphic loop $(Q, \circ)$, one can define a Bruck loop $(Q, \oplus \circ)$ on the same
underlying set $Q$ by

$$x \oplus_o y = (x^{-1} \odot (y^2 \circ x))^{1/2}. \quad (2.0.3)$$

Here $a \setminus_c b$ is the unique solution $c$ to $a \circ c = b$. We will extend this result to $\Gamma$-loops and thus obtain a functor from the category of uniquely 2-divisible $\Gamma$-loops to the category of uniquely 2-divisible Bruck loops, which restricts to a functor $\mathcal{B}: \Gamma L_{p_o} \hookrightarrow \text{BrL}_{p_o}$ from the category $\Gamma L_{p_o}$ of $\Gamma$-loops of odd order to the category $\text{BrL}_{p_o}$ of Bruck loops of odd order.

### 2.1 $\Gamma$-loops

It is not immediately obvious that $(G, \circ)$ is a loop. It is well-known in one special case. If $G$ is nilpotent of class at most 2, then $(G, \circ)$ is an abelian group (and in fact, coincides with $(G, \oplus)$). In this case, the passage from $G$ to $(G, \circ)$ is called the “Baer trick” [24]. In the general case, $(G, \circ)$ turns out to live in a variety of loops which we will call $\Gamma$-loops, on which we focus the rest of this chapter. For finite loops, we can characterize unique 2-divisibility in different ways.

**Theorem 2.1.1** ([26]). A finite commutative loop $Q$ is uniquely 2-divisible if and only if it has odd order. Similarly, a finite power-associative loop $Q$ is uniquely 2-divisible if and only if each element of $Q$ has odd order.

We now define a new variety of loops, $\Gamma$-loops. Note that by commutativity, $\Gamma$-loops have two-sided inverses.

**Definition 2.1.2.** A loop $(Q, \cdot)$ is a $\Gamma$-loop if the following hold

\[(\Gamma_1) \quad Q \text{ is commutative.}\]
(Γ₂) \( Q \) has the (AIP).

(Γ₃) \( \forall x \in Q, L_x L_{x^{-1}} = L_{x^{-1}} L_x \).

(Γ₄) \( \forall x, y \in Q, P_x P_y P_x = P_y P_x \) where \( P_x = R_x L_{x^{-1}} = L_{x^{-1}} R_x \).

Note that a loop satisfying the AIP necessarily satisfies \((x/y)^{-1} = x^{-1} y^{-1}\) and \((x/y)^{-1} = x^{-1}/y^{-1}\). We will use this without comment in what follows.

Our conventions for conjugation and commutators in groups are

\[ x^y = y^{-1} x y \quad \text{and} \quad [x, y] = x^{-1} y^{-1} x y = x^{-1} x^y = (y^{-1})x y. \]

The following identities are easily verified and will be used without reference.

**Lemma 2.1.3.** Let \( G \) be a group. Then for all \( x, y \in G \),

(i) \([x, y]^{-1} = [y, x]\)

(ii) \([x, y^{-1}] = [y, x]y^{-1} \) and \([x^{-1}, y] = [y, x]x^{-1}\),

(iii) \([xy, x^{-1}] = [x, yx^{-1}]\),

(iv) \([x^{-1}, y^{-1}] = [x, y](xy)^{-1}.\)

Moreover if \( G \) is uniquely 2-divisible,

(v) \((x^{1/2})^{-1} = (x^{-1})^{1/2},\)

(vi) \((x^y)^{1/2} = (x^{1/2})^y.\)

**Lemma 2.1.4.** Let \( G \) be a uniquely 2-divisible group. Then

(i) \( x \circ y = y \circ x,\)
(ii) \((x \circ y)^{-1} = x^{-1} \circ y^{-1}\),

(iii) \(xyx = \{x(y \circ x)x(y \circ x)^{-1}\}^{1/2}(y \circ x)\).

**Proof.** For (i), we have

\[
x \circ y = xy[y, y]^{1/2} = yx[x, y][y, x]^{1/2} = yx[x, y]([x, y]^{-1})^{1/2} = yx[x, y]^{1/2} = y \circ x.
\]

Similarly for (ii),

\[
x^{-1} \circ y^{-1} = x^{-1}y^{-1}[y^{-1}, x^{-1}]^{1/2} = (yx)^{-1}([y, x]^{(xy)^{-1}})^{1/2}
\]

\[
= (yx)^{-1}([y, x]^{1/2})^{(xy)^{-1}} = (yx)[y, x]^{1/2}(yx)^{-1}
\]

\[
= [y, x]^{1/2}(yx)^{-1} = ([x, y]^{-1})^{-1}(yx)^{-1}
\]

\[
= (yx[x, y]^{1/2})^{-1} = (y \circ x)^{-1}
\]

\[
= (x \circ y)^{-1}.
\]

For (iii), using (i) and (ii) from above,

\[
yx(y \circ x)^{-1} = yx(x^{-1} \circ y^{-1}) = yxx^{-1}y^{-1}[y^{-1}, x^{-1}]^{1/2}
\]

\[
= [y^{-1}, x^{-1}]^{1/2} = (xyy^{-1}xy^{-1}x^{-1})^{1/2}
\]

\[
= (xy[y, x]^{(xy)^{-1}})^{1/2} = xy[y, x]^{1/2}(xy)^{-1}
\]

\[
= (x \circ y)(xy)^{-1} = (y \circ x)^{-1}x^{-1}.
\]

Hence we have

\[
\{xy(x \circ x)^{-1}\}^2 = xy(x \circ x)^{-1}xy(x \circ x)^{-1} = x(y \circ x)^{-1}x^{-1}xy(x \circ x)^{-1}
\]

17
\[ = x(y \circ x)(y \circ x)^{-1}. \]

Thus \( xyx = \{x(y \circ x)(y \circ x)^{-1}\}^{1/2}(y \circ x), \) as claimed. \( \square \)

**Theorem 2.1.5.** Let \( G \) be a uniquely 2-divisible group. Then \( (G, \circ) \) is a \( \Gamma \)-loop.

**Proof.** To see \( (Q, \circ) \) is a loop, fix \( a, b \in Q \) and let \( x = \{a^{-1}ba^{-1}b\}^{1/2}b. \) Thus, we compute

\[
x = \{a^{-1}ba^{-1}b\}^{1/2}b \\
(xb^{-1})^2 = a^{-1}ba^{-1}b^{-1} \\
xb^{-1}x = a^{-1}ba^{-1} \\
xa = bx^{-1}a^{-1}b \\
[x, a] = (x^{-1}a^{-1}b)^2 \\
ax[x, a]^{1/2} = b \\
a \circ x = b.
\]

Note that this gives the following expression for \( \setminus \circ: \)

\[ a \setminus \circ b = \{a^{-1}ba^{-1}b\}^{1/2}b. \]

Moreover,

\[ 1 \circ x = 1x[x, 1]^{1/2} = x = x1[1, x]^{1/2} = x \circ 1 \]

and hence \( 1 \in Q \) is the neutral element in \( (Q, \circ). \) It is easy to see that inverses coincide in \( G \) and \( (G, \circ). \) Therefore, \( (\Gamma_1) \) and \( (\Gamma_2) \) are exactly Lemma 2.1.4(i) and
(ii). For \((\Gamma_3)\), first note

\begin{equation}
\tag{2.1.1}
\left( x^{(-1)} \circ (xy) \right) = \left[ xy, x^{(-1)} \right]^{1/2} = \left[ x, yx^{(-1)} \right]^{1/2} = \left( yx^{(-1)} \right) \circ x = x \circ (yx^{(-1)}).
\end{equation}

Similarly,

\begin{equation}
\tag{2.1.2}
x^{-1} \circ y = x^{-1}y\left[ y, x^{-1} \right]^{1/2} = x^{-1}y\left[ x, y \right]^{1/2}x^{-1} = y\left[ y, x \right]^{1/2}x^{-1}.
\end{equation}

Therefore

\begin{equation}
\tag{2.1.3}
x^{-1} \circ (x \circ y) = x^{-1} \circ (xy\left[ y, x \right]^{1/2}) = x \circ ((y\left[ y, x \right]^{1/2})x^{-1}) = x \circ (x^{-1} \circ y).
\end{equation}

For \((\Gamma_4)\), rewriting Lemma 2.1.4(iii) gives

\begin{equation}
\tag{2.1.4}
xyx = \left\{ x(y \circ x)x(y \circ x)^{-1} \right\}^{1/2}(y \circ x) = x^{-1}(y \circ x) = yP_x.
\end{equation}

Let \(y \Psi_x = xyx\), that is, \(y \Psi_x = yP_x\). Hence, \(P_xP_yP_x = \Psi_x \Psi_y \Psi_x = \Psi_y \Psi_x = P_yP_x\).

**Lemma 2.1.6.** Commutative automorphic loops are \(\Gamma\)-loops.

**Proof.** This follows from Lemmas 2.6, 2.7 and 3.3 in [26].

**Example 2.1.7.** The smallest known \(\Gamma\)-loop constructed from a group of odd order has order 375, and its underlying group is the smallest group of odd order that is not metabelian, with GAP library number \([375; 2]\). Later we will show an example of a subloop of order 75 which is also not automorphic, and that subloop is the smallest known nonautomorphic \(\Gamma\)-loop of odd order.

**Example 2.1.8.** The following is the smallest \(\Gamma\)-loop which is neither a commutative
automorphic nor commutative semiautomorphic loop, found by MACE4 [37].

\[
\begin{array}{c|ccccc}
\cdot & 0 & 1 & 2 & 3 & 4 & 5 \\
0 & 0 & 1 & 2 & 3 & 4 & 5 \\
1 & 1 & 0 & 3 & 5 & 2 & 4 \\
2 & 2 & 3 & 0 & 4 & 5 & 1 \\
3 & 3 & 5 & 4 & 0 & 1 & 2 \\
4 & 4 & 2 & 5 & 1 & 0 & 3 \\
5 & 5 & 4 & 1 & 2 & 3 & 0 \\
\end{array}
\]

Table 2.1: The smallest $\Gamma$-loop

\section{2.2 $\Gamma$-Loops are power-associative}

Recall our definition $x^n = 1L^n_x$ for all $n \in \mathbb{Z}$.

\textbf{Proposition 2.2.1.} Let $Q$ be a $\Gamma$-loop. Then $x^{-n} = (x^{-1})^n = (x^n)^{-1}$.

\textbf{Proof.} The first equality, $(1)L_{x^{-n}} = (1)L^n_{x^{-1}}$, is equivalent to $1 = (1)L^n_{x^{-1}}L^n_x$. By $(\Gamma_3)$, $L^n_{x^{-1}}L^n_x = (L_{x^{-1}}L_x)^n$. But since $L_{x^{-1}}L_x \in \text{Inn}(Q)$, we are done. The second equality follows from $(\Gamma_2)$. \hfill \Box

\textbf{Proposition 2.2.2.} Let $Q$ be a $\Gamma$-loop. Then

\[P_x = L_xL^{-1}_{x^{-1}} = L^{-1}_{x^{-1}}L_x \quad (P_1)\]

\[P_xL_x = L_xP_x \quad (P_2)\]

\textbf{Proof.} These follow from $(\Gamma_3)$. \hfill \Box

\textbf{Lemma 2.2.3.} Let $Q$ be a $\Gamma$-loop. Then $\forall k, n \in \mathbb{Z}$ we have the following:

\begin{enumerate}
\item[(a)] $x^n P_x = x^{n+2}$
\end{enumerate}
(b) \( P^n_x = P_x^n \)

(c) \( x^k P_x^n = x^{k+2n} \)

**Proof.** Note that \( 1P_x = x^2 \) by \((\Gamma_3)\). For all \( n \), we have

\[
X^n P_x = 1L^n_x P_x \overset{(P_2)}= 1P_x L^n_x = x^2 L^n_x = x P_{x^n} = x^{n+2}. 
\]

For (b), the cases \( n = 0, 1 \) are trivially true. For \( n > 1 \),

\[
P^n_x = P_xP^{n-2}_x = P_xP_x^{n-2}P_x \overset{(\Gamma_4)}= P_{x^{n-2}}P_x \overset{(a)}= P_x^n. 
\]

If \( n = -1 \) then \( P_{x^{-1}} = L_{x^{-1}}L_{x^{-1}} = (L_xL_{x^{-1}})^{-1} = P_{x^{-1}} \). Thus we have for any \( n < 0 \),

\[
P^n_x = (P_x^{-n})^{-1} = P_{x^{-n}} = P_{(x^{-n})^{-1}} = P_x^n, 
\]

by Proposition 2.2.1.

For (c), let \( k \) be fixed. Then

\[
x^k P_x^n \overset{(b)}= x^k P_x^n \overset{(a)}= x^{k+2} P_x^{n-1} \overset{(a)}= \ldots \overset{(a)}= x^{k+2n}. 
\]

For \( m \in \mathbb{N}_0 = \mathbb{N} \cup \{0\} \), we define \( PA(m) \) to be the statement:

\[
\forall i \in \{-m,\ldots,m\} \text{ and } \forall j \in \{-m-1,\ldots,m+1\}, \quad x^i x^j = x^{i+j}. 
\]

**Lemma 2.2.4.** Let \( Q \) be a \( \Gamma \)-loop. Then \( PA(m) \) holds for all \( m \in \mathbb{N}_0 \).

**Proof.** We induct on \( m \). \( PA(0) \) is obvious. Assume \( PA(m) \) holds for some \( m \geq 0 \). We establish \( PA(m+1) \) by proving \( x^i x^j = x^{i+j} \) for each of the following cases:
\[(1) \quad i \in \{-m - 1, \ldots, m + 1\}, \quad j \in \{-m, \ldots, m\}, \]

\[(2) \quad i \in \{-m, \ldots, m\}, \quad j = m + 1 \quad \text{or} \quad j = -m - 1, \]

\[(3) \quad i = m + 1, \quad j = -m - 1 \quad \text{or} \quad i = -m - 1, \quad j = m + 1, \]

\[(4) \quad i = m + 1, \quad j = m + 1 \quad \text{or} \quad i = -m - 1, \quad j = -m - 1, \]

\[(5) \quad i \in \{-m - 1, \ldots, m + 1\}, \quad j = m + 2 \quad \text{or} \quad j = -m - 2. \]

By \((\Gamma_2)\) and Proposition 2.2.1, \(x^i x^j = x^{i+j}\) implies \(x^{-i} x^{-j} = x^{-i-j}\). So in each of cases (2), (3), (4) and (5), we only need to establish one of the subcases.

Case (1) follows from \(\text{PA}(m)\) (with the roles of \(i\) and \(j\) reversed) and commutativity. Case (2) also follows from \(\text{PA}(m)\). Case (3) follows from Proposition 2.2.1:

\[x^{m+1} x^{m-1} = x^{m+1} x^{-(m+1)} = 1.\]

For case (4),

\[x^{m+1} x^{m+1} = (1)_{L^{-1}_{x^{-m+1}} L_{x^{m+1}}} (P_1)_{x^{m+1}} (2.2.3c) \equiv x^{2m+2}.\]

Finally, for case (5), first suppose \(i \in \{-m - 1, \ldots, -1\}\). Then \(-2m - 2 \leq 2i \leq -2\), and so \(-m \leq m + 2 + 2i \leq m\), that is, \(m + 2 + 2i \in \{-m, \ldots, m\}\). Thus

\[x^i x^{m+2} = (x^{m+2})_{x^i} L_{x^{-i}} (2.2.3c) x^{-i} x^{m+2+2i} \equiv \text{PA}(m) x^{m+2+i}.\]

Now suppose \(i \in \{1, \ldots, m + 1\}\). Then \(-2m - 2 \leq -i \leq -2\), and so \(-m \leq m + 2 - 2i \leq m\), that is, \(m + i - 2i \in \{-m, \ldots, m\}\). Thus

\[x^i x^{m+2} (2.2.3c) \equiv (x^{m+2-2i})_{x^i} L_{x^{-i}} (P_1)_{x^i} (x^i x^{m+2-2i})_{x^i} \equiv \text{PA}(m) x^{m+2+i}.\]

\[\square\]
**Theorem 2.2.5.** Γ-loops are power-associative.

*Proof.* This follows immediately from Lemma 2.2.4. Indeed, \( x^k x^\ell = x^{k+\ell} \) with \( 0 \leq |k| \leq |\ell| \) follows from PA(\(|\ell|\)). □

By Theorem 2.1.5 and Theorem 2.2.5, for a uniquely 2-divisible group \( G \) and its corresponding Γ-loop \((G, \circ)\), we have powers coinciding.

**Corollary 2.2.6.** Let \( G \) be a uniquely 2-divisible group and \((G, \circ)\) its associated Γ-loop. Then powers in \( G \) coincide with powers in \((G, \circ)\).

### 2.3 Twisted subgroups and uniquely 2-divisible Bruck loops

In this section, we first review the notion of twisted subgroup of a group and the connection between uniquely 2-divisible twisted subgroups and uniquely 2-divisible Bruck loops. We follow the notations and definitions used by Foguel, Kinyon and Phillips [16], and refer the reader to that paper for a more complete discussion of the following results.

**Definition 2.3.1.** A twisted subgroup of a group \( G \) is a subset \( T \subseteq G \) such that \( 1 \in T \) and for all \( x, y \in T \), \( x^{-1} \in T \) and \( xyx \in T \).

**Example 2.3.2 ([16]).** Let \( G \) be a group and \( \tau \in \text{Aut}(G) \) with \( \tau^2 = 1 \). Let \( K(\tau) = \{ g \in Q \mid g\tau = g^{-1} \} \). Then \( K(\tau) \) is a twisted subgroup.

**Proposition 2.3.3.** Let \( G \) be uniquely 2-divisible group and let \( \tau \in \text{Aut}(G) \) satisfy \( \tau^2 = 1 \). Then \( K(\tau) \) is closed under \( \circ \) and \( \setminus \) and hence is a subloop of \((G, \circ)\).
Proof. Let \( x, y \in K(\tau) \). Then

\[
(x \circ y)\tau = (xy[y, x]^{1/2})\tau = x\tau y\tau[y\tau, x\tau]^{1/2} = x^{-1}y^{-1}[y^{-1}, x^{-1}]^{1/2} = x^{-1} \circ y^{-1} = (x \circ y)^{-1}
\]

by \((\Gamma_2)\). Similarly, \((\Gamma_2)\) also gives \((x \setminus_\circ y)\tau = (x \setminus_\circ y)^{-1}\).

\[\square\]

**Theorem 2.3.4** ([16]). Let \( Q \) be a Bruck loop. Then \( L_Q \) is a twisted subgroup of \( \text{Mlt}_\lambda(Q) \). If \( Q \) has odd order, then \( \text{Mlt}_\lambda(Q) \) has odd order. Moreover, there exists a unique \( \tau \in \text{Aut}(\text{Mlt}_\lambda(Q)) \) where \( \tau^2 = 1 \) and \( L_Q = \{ \theta \in \text{Mlt}_\lambda(Q) \mid \theta \tau = \theta^{-1} \} \). On generators, \((L_\lambda)^\tau = L_{\lambda^{-1}}\).

**Corollary 2.3.5.** Let \((Q, \cdot)\) be a Bruck loop of odd order. Then \((L_Q, \circ)\) is a \( \Gamma \)-loop.

**Proof.** This follows from Proposition 2.3.3 and Theorem 2.3.4. \[\square\]

We have a bijection from \( L_Q \) to \( Q \) given by \( L_\lambda \mapsto 1L_\lambda = x \). This allows us to define a \( \Gamma \)-loop operation directly on \( Q \) as follows:

\[
x \circ y = 1(L_\lambda \circ L_y)
\]

where we reuse the same symbol \( \circ \). By construction, the \( \Gamma \)-loops \((L_Q, \circ)\) and \((Q, \cdot)\) are isomorphic.

**Proposition 2.3.6.** Let \((Q, \cdot)\) be a Bruck loop of odd order. Then \((Q, \circ)\) is a \( \Gamma \)-loop. Moreover, powers in \((Q, \circ)\) coincide with powers in \((Q, \cdot)\).

**Proof.** For powers coinciding, suppose \( x^n \) denotes powers in \((Q, \cdot)\). Since Bruck loops are left power-alternative [44], \( x^n = 1L_\lambda x^n = 1L_x^n \). By Corollary 2.2.6, \( L_x^n \) coin-
cides with the \( n \)th power of \( L_x \) in \( (L_Q, \circ) \). Thus \( x^n \) is the \( n \)th power of \( x \) in \( (Q, \circ) \). Since this argument is clearly reversible, we have the desired result.

The following example shows that finiteness is needed in order to construct a \( \Gamma \)-loop \( (Q, \circ) \) from a Bruck loop \( (Q, \cdot) \), ensuring that square roots make sense in \( \text{Mlt}_\lambda(Q) \).

**Example 2.3.7** ([31]). Let \( Q \) be the set of real positive definite \( 2 \times 2 \) matrices. Then \( (Q, \oplus) \) is a uniquely 2-divisible Bruck loop and \( L_Q \) is a uniquely 2-divisible twisted subgroup of \( \text{Mlt}_\lambda(Q) \). However, \( \text{Mlt}_\lambda(Q) = PSL(2, \mathbb{R}) \), which is not a uniquely 2-divisible group.

For a uniquely 2-divisible \( \Gamma \)-loop \( (Q, \cdot) \), we set

\[
\begin{align*}
x \oplus y &= (x^{-1} \cdot (y^2 x))^{1/2},
\end{align*}
\]

and if \( \circ \) is another \( \Gamma \)-loop operation on the same underlying set, we similarly define \( \oplus_\circ \). Our next goal is to generalize Lemma 3.5 of [26] and show that \( (Q, \oplus) \) is a Bruck loop.

**Lemma 2.3.8.** Let \( Q \) be a \( \Gamma \)-loop. Then

\[
(yP_x)^2 = x^2 P_y P_x.
\]

**Proof.** By Proposition 2.2.3(a), we have that \( x^2 = 1P_x \). Hence,

\[
x^2 P_y P_x = 1P_x P_y P_x \overset{(\Gamma_4)}{=} 1P_y P_x = (yP_x)^2
\]
by Proposition 2.2.3(a) again. □

**Theorem 2.3.9.** Let \((Q, \cdot)\) be a uniquely 2-divisible \(\Gamma\)-loop. Then \((Q, \circ)\) is a Bruck loop. Moreover, powers in \((Q, \cdot)\) coincide with powers in \((Q, \circ)\).

**Proof.** Note that \((x \circ (y \circ x)) \circ z = x \circ (y \circ (x \circ z))\) is equivalent to \(\lambda_x \lambda_y \lambda_z = \lambda_{x \circ (y \circ z)}\) where \(y \lambda_x = x \circ y\). Let \(x \delta = x^2\). Then \(y \lambda_x = x \circ y = (x^{-1} \cdot (y^2 x))^{1/2} = y \delta P_x \delta^{-1}\). Thus,

\[
\lambda_x \lambda_y \lambda_z = \delta P_x \delta^{-1} \delta P_y \delta^{-1} \delta P_z \delta^{-1} = \delta P_x \circ P_y \circ P_z \delta^{-1} = \delta P_y \circ P_x \delta^{-1}.
\]

But by Proposition 2.3.8,

\[
y P_x = (x^2 P_y P_x)^{1/2} = (x^{-1} \cdot [(y^{-1} \cdot (x^2 y)) x])^{1/2} = x \circ (y^{-1} \cdot (x^2 y))^{1/2} = x \circ (y \circ x).
\]

Thus,

\[
\lambda_x \lambda_y \lambda_z = \delta P_y P_x \delta^{-1} = \delta P_{x \circ (y \circ x)} \delta^{-1} = \lambda_{x \circ (y \circ x)}.
\]

The fact that \((Q, \circ)\) has AIP is straightforward from \((\Gamma_2)\). Powers coinciding follows from power-associativity of \((Q, \cdot)\) and \((Q, \circ)\). □

We now have a construction of \(\Gamma\)-loops from Bruck loops and a construction of Bruck loops from \(\Gamma\)-loops. In the next section, we will show that when we iterate these constructions, we get nothing new, but in the meantime, we will use the following notation conventions. Our “starting loop” will always be denoted by \((Q, \cdot)\). The Bruck loops constructed from a particular \(\Gamma\)-loop operation will be distinguished by subscripts. The \(\Gamma\)-loop operation constructed from any Bruck loop will be denoted simply by \(\circ\); as it turns out, we will not need to construct \(\Gamma\)-loops.
for (seemingly) distinct Bruck loops.

So for instance, if we start with a Bruck loop, construct a $\Gamma$-loop and then another Bruck loop, we will follow this sequence:

$$(Q, \cdot) \rightsquigarrow (Q, \circ) \rightsquigarrow (Q, \oplus \circ).$$

If we start with a $\Gamma$-loop, construct a Bruck loop and then a $\Gamma$-loop, we will follow this sequence:

$$(Q, \cdot) \rightsquigarrow (Q, \oplus) \rightsquigarrow (Q, \circ).$$

All of this is just a temporary inconvenience, as our goal in the next section is to show that the starting and ending loops in both sequences are not only isomorphic, they are in fact identical.

Given a Bruck loop $(Q, \cdot)$ of odd order, we wish to give the explicit equation of the left division (and hence right division by commutativity) operation in $(Q, \circ)$. We will need the following two facts for Bol loops, both well known.

**Proposition 2.3.10** ([17, 44]). *In a Bruck loop $Q$, the identity $(xy)^2 = x \cdot y^2 x$ holds for all $x, y \in Q$.***

**Proposition 2.3.11.** Let $(Q, \cdot)$ be a Bruck loop of odd order and let $(Q, \circ)$ be its $\Gamma$-loop. For all $a, b \in Q$.

$$b / \circ a = (a^{-1}b^{1/2}) / b^{-1/2}.$$

*Proof.* Let $a, b \in Q$ be fixed and set $x = (a^{-1}b^{1/2}) / b^{-1/2}$. Then $xb^{-1/2} = a^{-1}b^{1/2}$. 

27
Squaring both sides gives
\[ x \cdot b^{-1}x = a^{-1} \cdot ba^{-1} \]

using Proposition 2.3.10. But this is equivalent to \( L_{x \cdot b^{-1}x} = L_{a^{-1} \cdot ba^{-1}} \) and since \((Q, \cdot)\) is a Bruck loop, we have \( L_{x \cdot b^{-1}x} = L_{a^{-1} \cdot ba^{-1}} \). This in turn is equivalent to \([L_{a}, L_{x}] = (L_{a}^{-1} L_{x}^{-1} L_{b})^{2}\) and therefore \( L_{x \cdot a} [L_{a}, L_{x}]^{1/2} = L_{b} \). That is, \( L_{x \circ a} = L_{b} \).

Hence, \( 1 (L_{x \circ a}) = 1 L_{b} \) and so \( x \circ a = b \).

Let \((G, \cdot)\) be a uniquely 2-divisible group. We have its Bruck loop \((G, \oplus)\) and also the Bruck loop \((G, \oplus \circ)\) of the \(\Gamma\)-loop \((G, \circ)\). We now show these coincide.

**Theorem 2.3.12.** Let \((G, \cdot)\) be a uniquely 2-divisible group. Then \((G, \oplus) = (G, \oplus \circ)\).

**Proof.** Recall (2.1.3) from Theorem 2.1.5, we have \( xyx = yP_{x} \) for all \( x, y \in G \). Replacing \( y \) by \( y^{2} \) and applying square roots gives \( x \oplus y = (xy^{2}x)^{1/2} = (y^{2}P_{x})^{1/2} = (x^{-1} \circ (y^{2} \circ x))^{1/2} = x \oplus \circ y \).

**Corollary 2.3.13.** Let \((G, \cdot)\) be a uniquely 2-divisible group, let \((H, \circ) \leq (G, \circ)\) and suppose that \( H \) is closed under taking square roots. Then \( H \) is a twisted subgroup of \( G \). In particular, if \( G \) is a finite group of odd order and \((H, \circ) \leq (G, \circ)\), then \( H \) is a twisted subgroup of \( G \).

**Proof.** Again, from (2.1.3) in Theorem 2.1.5, we have \( xyx = yP_{x} = (x^{-1} \circ (y \circ x))^{1/2} \in H \) for all \( x, y \in H \). Finally, since powers coincide in \( H \) and \((H, \circ), x^{-1} \in H \).

**Example 2.3.14.** Let \( G \) be the smallest nonmetabelian group of odd order from Example 2.1.7. Then there exists a twisted subgroup \( H \) of \( G \) with \( |H| = 75 \). Here \((H, \circ)\) is the smallest known example of a nonautomorphic \(\Gamma\)-loop of odd order.
2.4 Inverse functors

We turn to our main results which is showing the newly constructed functor \( \mathcal{G} : \text{BrL}_p \to \Gamma \text{L}_p \) is the inverse functor of \( \mathcal{B} \). That is, \( \mathcal{G} \circ \mathcal{B} \) is the identity functor on \( \Gamma \text{L}_p \) and \( \mathcal{B} \circ \mathcal{G} \) is the identity functor on \( \text{BrL}_p \). We will need the following lemma for our main result.

**Lemma 2.4.1.** Let \((Q, \cdot)\) be a uniquely 2-divisible \( \Gamma \)-loop and \((Q, \oplus)\) be its Bruck loop. Then

\[
x \oplus (xy)^{-1/2} = y^{-1} \oplus (xy)^{1/2}.
\]  

(2.4.1)

**Proof.** First note that \( x \oplus (xy)^{-1/2} = y^{-1} \oplus (xy)^{1/2} \iff x^{-1}(x^{-1}y^{-1} \cdot x) = y(x \cdot y^{-1}) \). Therefore we compute

\[
x^{-1}(x^{-1}y^{-1} \cdot x) \overset{(\Gamma_1)}{=} x^{-1}(x \cdot x^{-1}y^{-1}) \overset{(\Gamma_3)}{=} x^{-1}(x^{-1} \cdot xy^{-1}) = xy^{-1} \overset{(\Gamma_1)}{=} y^{-1}x = y(y \cdot y^{-1}x) \overset{(\Gamma_3)}{=} y(y^{-1} \cdot yy) \overset{(\Gamma_1)}{=} y(yy \cdot y^{-1})
\]

Now let \( \mathcal{G} : \text{BrL}_p \to \Gamma \text{L}_p \) be the functor given on objects by assigning to each Bruck loop of odd order \((Q, \cdot)\) its corresponding \( \Gamma \)-loop \((Q, \circ)\), and let \( \mathcal{B} : \Gamma \text{L}_p \to \text{BrL}_p \) be the functor given on objects by assigning to each \( \Gamma \)-loop of odd order \((Q, \cdot)\) its corresponding Bruck loop \((Q, \oplus)\).

Note that both categories are defined as a variety of finite loops of odd order. We claim the morphisms in both categories are homomorphisms. Indeed, it is clear that finiteness is preserved under homomorphisms. For unique square roots, suppose...
\[ \theta : Q_1 \mapsto Q_2 \] is a loop homomorphism in either category. Then

\[
(x^{1/2} \theta)^2 = (x^{1/2})^2 \theta = x \theta.
\]

Thus, taking square roots in \( Q_2 \), we have \( x^{1/2} \theta = (x \theta)^{1/2} \). Therefore, any loop homomorphism in either category preserves square roots. Moreover, the functors in either direction preserve powers, hence are functors not only of finite loops, but finite loops with unique square roots.

**Theorem 2.4.2.**

(A) \( \mathcal{B} \circ \mathcal{F} \) is the identity functor on \( \Gamma Lp_o \).

(B) \( \mathcal{F} \circ \mathcal{B} \) is the identity functor on \( BrLp_o \).

**Proof.** (A) Let \((Q, \cdot)\) be a \( \Gamma \)-loop of odd order, let \((Q, \oplus)\) be its corresponding Bruck loop and let \((Q, \circ)\) be the \( \Gamma \)-loop of \((Q, \oplus)\). Lemma 2.4.1 and Proposition 2.3.11 imply

\[
x = (x \oplus (xy)^{-1/2})/\oplus (xy)^{-1/2} = (y^{-1} \oplus (xy)^{1/2})/\oplus (xy)^{-1/2} = (xy)/_o y.
\]

Thus \( xy = x \circ y \), as claimed.

(B) Let \((Q, \cdot)\) be a Bruck loop of odd order, let \((Q, \circ)\) be its corresponding \( \Gamma \)-loop and let \((Q, \oplus_o)\) be the Bruck loop of \((Q, \circ)\). Recalling that the map \( x \mapsto L_x \) (left translations in \((Q, \cdot)\)) is an isomorphism of \((Q, \circ)\) with \((L_Q, \circ)\), we have

\[
L_{(x \oplus y)^2} = L_{x^{-1} \circ (y^2 \circ x)} = L_{x^{-1} \circ (L_y^2 \circ L_x)} = (L_x \oplus_o L_y)^2 = (L_x \oplus L_y)^2 = L_{x \cdot (y^2, x)}
\]
\[ L((xy)^2), \]

using Theorem 2.3.12 and Proposition 2.3.10. Thus \((xy)^2 = (x \oplus_o y)^2\) and so the desired result follows from taking square roots. \(\square\)

We note in passing that we have proven a result which can be stated purely in terms of Bruck loops of odd order:

*Let \((Q, \cdot)\) be a Bruck loop of odd order. For each \(x, y \in Q\), the equation*

\[ xz^{-1/2} = y^{-1}z^{1/2} \]

*has a unique solution \(z \in Q\). Indeed, \(z = x \circ y\) where \((Q, \circ)\) is the \(\Gamma\)-loop of \((Q, \cdot)\).*

We conclude this section by discussing the intersection of the varieties of Bruck loops and \(\Gamma\)-loops.

**Proposition 2.4.3.** A loop is both a Bruck loop and \(\Gamma\)-loop if and only if it is a commutative Moufang loop.

**Proof.** The “if” direction is clear. For the converse, commutative Bruck loops are commutative Moufang loops [45]. \(\square\)

The following result quickly follows from the fact that Moufang loops are diassociative (i.e. the subloop \(\langle x, y \rangle\) is a group for all \(x, y\)) and the definitions of the operations.

**Proposition 2.4.4.** Let \((Q, \cdot)\) be a uniquely 2-divisible commutative Moufang loop. Then \((Q, \cdot) = (Q, \circ) = (Q, \oplus).\)

**Proposition 2.4.5.** Let \((Q, \cdot)\) be a \(\Gamma\)-loop of exponent 3. Then \((Q, \cdot)\) is a commutative Moufang loop.
Proof. The associated Bruck loop \((Q, \oplus)\) is a commutative Moufang loop [45]. Moreover, recalling Proposition 2.4.1, \(x \oplus (xy)^{-1/2} = y^{-1} \oplus (xy)^{1/2}\) holds for all \(x, y \in Q\). Hence, using diassociativity, we have

\[
x = (y^{-1} \oplus (xy)^{1/2}) \oplus (xy)^{1/2} = y^{-1} \oplus (xy).
\]

Thus, \(xy = y \oplus x = x \oplus y\), and therefore, \((Q, \cdot) = (Q, \oplus)\) is a commutative Moufang loop.

\section{2.5 \(\Gamma\)-loops of odd order}

Finite Bruck loops of odd order are known to have many remarkable properties, all found by Glauberman [17, 18]. For instance, they satisfy Lagrange’s Theorem, the Odd Order Theorem, the Sylow and Hall Existence Theorems and finite Bruck \(p\)-loops \((p\ \text{odd})\) are centrally nilpotent. Using the isomorphism of the categories \(\Gamma\text{Lp}_0\) and \(\text{BrLp}_0\), we immediately get the same results for \(\Gamma\)-loops of odd order.

We will take notational advantage of Theorem 2.4.2 and write simply \(\oplus\) for the Bruck loop operation of a \(\Gamma\)-loop of odd order.

**Proposition 2.5.1.** Let \((Q, \cdot)\) be a \(\Gamma\)-loop with \(|Q| = p^2\) for \(p\) prime. Then \((Q, \cdot)\) is an abelian group.

**Proof.** Loops of order 4 are abelian groups [42], so assume \(p > 2\). For odd primes, Bruck loops of order \(p^2\) are abelian groups [10]. Thus since \((Q, \oplus)\) is an abelian group, so is its \(\Gamma\)-loop, which, by Theorem 2.4.2, coincides with \((Q, \cdot)\).

**Lemma 2.5.2.** Let \((Q, \cdot)\) be a \(\Gamma\)-loop of odd order and let \((Q, \oplus)\) be its Bruck loop. Then the derived subloops of \((Q, \cdot)\) and \((Q, \oplus)\) coincide. In particular, the derived
series of \((Q, \cdot)\) and \((Q, \oplus)\) coincide.

Proof. By the categorical isomorphism (Theorem 2.4.2), any normal subloop of \((Q, \oplus)\) is a normal subloop of \((Q, \cdot)\) and vice versa, since normal subloops are kernels of homomorphisms [8]. If \(S\) is the derived subloop of \((Q, \oplus)\), then \(S\) is a normal subloop of \((Q, \cdot)\) such that \((Q/S, \cdot)\) is an abelian group. If \(M\) were a smaller normal subloop of \((Q, \cdot)\) with this property, then it would have the same property for \((Q, \oplus)\), a contradiction. The converse is proven similarly. \(\square\)

Theorem 2.5.3 (Odd Order Theorem). \(\Gamma\)-loops of odd order are solvable.

Proof. Let \((Q, \cdot)\) be a \(\Gamma\)-loop of odd order and let \((Q, \oplus)\) be its Bruck loop. Then \((Q, \oplus)\) is solvable ([18], Theorem 14(b), p. 412), and so the desired result follows from Lemma 2.5.2. \(\square\)

Theorem 2.5.4 (Lagrange and Cauchy Theorems). Let \((Q, \cdot)\) be a \(\Gamma\)-loop of odd order. Then:

\(\text{(L)}\) If \(A \leq B \leq Q\) then \(|A|\) divides \(|B|\).

\(\text{(C)}\) If an odd prime \(p\) divides \(|Q|\), then \(Q\) has an element an order of \(p\).

Proof. Both subloops \(A\) and \(B\) give subloops \((A, \oplus)\) and \((B, \oplus)\) of \((Q, \oplus)\). The result follows from ([17], Corollary 4, p. 395). Similarly, if an odd prime \(p\) divides \(|Q|\), then \((Q, \oplus)\) has an element of order \(p\) ([17], Corollary 1, p. 394). Hence, \(Q\) has an element of order \(p\). \(\square\)

Theorem 2.5.5. Let \(Q\) be a \(\Gamma\)-loop of odd order and let \(p\) be an odd prime. Then \(|Q|\) is a power of \(p\) if and only if every element of \(Q\) has order a power of \(p\).
Remark 2.5.6. Note that this is false for $p = 2$ by Example 2.1.8.

Proof. If $|Q|$ is a power of $p$, then by Theorem 2.5.4(L) every element has order a power of $p$. On the other hand, if $|Q|$ is divisible by an odd prime $q$, then by Theorem 2.5.4(C), $Q$ contains an element of order $q$. Therefore, if every element is order $p$, $|Q|$ must have order a power of $p$.

Thus, in the odd order case, we can define $p$-subloops of $\Gamma$-loops. Moreover, we can now show the existence of Hall $\pi$-subloops and Sylow $p$-subloops.

Theorem 2.5.7 (Sylow subloops). $\Gamma$-loops of odd order have Sylow $p$-subloops.

Proof. Let $(Q, \cdot)$ be a $\Gamma$-loop of odd order and $(Q, \oplus)$ its Bruck loop. Then $(Q, \oplus)$ has a Sylow $p$-subloop ([17], Corollary 3, p. 394), say $(P, \oplus)$. But then $(P, \circ)$ is a Sylow $p$-subloop of $(Q, \cdot)$ by Theorem 2.4.2.

Theorem 2.5.8 (Hall subloops). $\Gamma$-loops of odd order have Hall $\pi$-subloops.

Proof. Let $(Q, \cdot)$ be a $\Gamma$-loop of odd order and $(Q, \oplus)$ its Bruck loop. Then $(Q, \oplus)$ has a Hall $\pi$-subloop ([17], Theorem 8, p. 392), say $(H, \oplus)$. But then $(H, \circ)$ is a Hall $\pi$-subloop of $(Q, \cdot)$ by Theorem 2.4.2.

Theorem 2.5.9. Let $(Q, \cdot)$ be a Bruck loop of odd order. Then $Z(Q, \cdot) = Z(Q, \circ)$.

Proof. Let $a \in Z(Q, \cdot)$ and recall $a(a \circ x)^{-1/2} = x^{-1}(a \circ x)^{1/2}$ from Lemma 2.4.1 holds for any $x \in Q$. Then

$$x \cdot a(a \circ x)^{-1/2} = (a \circ x)^{1/2} \Leftrightarrow xa \cdot (a \circ x)^{-1/2} = (a \circ x)^{1/2} \Leftrightarrow xa = a \circ x.$$ 

Moreover, for any $x, y, z \in Q$,

$$z[L_y, L_{xa}] = zL_y^{-1}L_{xa}^{-1}L_yL_{xa} = xa \cdot y((xa)^{-1} \cdot y^{-1}z) = x \cdot y(x^{-1} \cdot y^{-1}z) = z[L_y, L_x].$$
Thus, for all $x, y \in Q$, noting $L_{ax} = L_a L_x$,

$$(a \circ x) \circ y = ax \circ y = L_{ax} \circ L_y = L_a L_x \circ L_y$$

$$= L_a L_x L_y [L_y, L_a L_x]^{1/2} = L_a L_x L_y [L_y, L_x]^{1/2} = L_a L_{xy}$$

$$= L_{a(xy)} = L_{a \circ (xy)} = a \circ (x \circ y).$$

Therefore $a \in Z(Q, \circ)$ by commutativity of $(Q, \circ)$. Similarly, let $a \in Z(Q, \circ)$ and let $(Q, \oplus)$ be its corresponding Bruck loop. It is enough to show that $ax = xa$ and $xa \cdot y = x \cdot ay$ since in a Bruck loop, $xa \cdot y = x \cdot ay \iff a \cdot xy = ax \cdot y$. We compute

$$ay = a \oplus y = (a^{-1} \circ (y^2 \circ a))^{1/2} = (a^2 \circ y^2)^{1/2} = a \circ y = y \circ a = ya.$$

Moreover,

$$xa \cdot y = xa \oplus y = ((xa)^{-1} \circ (y^2 \circ (xa)))^{1/2} = ((x \circ a)^{-1} \circ (y^2 \circ (x \circ a)))^{1/2}$$

$$= (x^{-1} \circ ((a \circ y)^2 \circ x))^{1/2} = x \oplus (ay) = x \cdot ay.$$

Therefore $a \in Z(Q, \cdot)$.

Define $Z_0(Q) = 1$ and $Z_{n+1}(Q), n \geq 0$ as the preimage of $Z(Q/Z_n(Q))$ under the natural projection. This defines the upper central series

$$1 \leq Z_1(Q) \leq Z_2(Q) \leq \ldots \leq Z_n(Q) \leq \ldots \leq Q$$

of $Q$. If for some $n$ we have $Z_{n-1}(Q) < Z_n(Q) = Q$, then $Q$ is said to be (centrally) nilpotent of class $n$. 
Theorem 2.5.10. Let \( p \) be an odd prime. Then finite \( \Gamma p \)-loops are centrally nilpotent.

Proof. Since \( Z(Q, \cdot) = Z(Q, \oplus) \), it follows by induction that \( Z_n(Q, \cdot) = Z_n(Q, \oplus) \) for all \( n > 0 \). But \( (Q, \oplus) \) is centrally nilpotent of class, say, \( n \) ([17], Theorem 7, p. 390). Therefore, \( (Q, \cdot) \) is centrally nilpotent of class \( n \). \( \square \)

2.6 Constructing commutative automorphic loops

One can certainly wonder when \((G, \circ)\) constructs a commutative automorphic loop. Let \( G \) be a uniquely 2-divisible, non-abelian group and with \(|G| = pq\) where \( p, q \) are odd primes and \( p|(q - 1) \). Then \( G \cong \mathbb{Z}_p \times \mathbb{Z}_q \) where \( \mathbb{Z}_p \leq \mathbb{Z}_q^* \) with multiplication in \( G \) defined by \((a, b)(c, d) = (a + bc, bd)\) for some \( a, c \in \mathbb{Z}_p \) and \( b, d \in \mathbb{Z}_q \).

For ease of calculations, we have the following.

Lemma 2.6.1. Let \( x, y \in G \), with \( x = (a, b), y = (c, d) \). Then

(i) \((0, 1)\) is the identity in \( G \),

(ii) \( x^{-1} = (-b^{-1}a, b^{-1}) \) and

(iii) \( x^{1/2} = \left(\frac{a}{1 + b^{2q}}, b^{2q}\right) \).

Proof. Let \( x, y \in G \) with \( x = (a, b), y = (c, d) \) as before. For (i),

\[(0, 1)(a, b) = (0 + 1(a), 1(b)) = (a, b).\]

For (ii), we have

\[xx^{-1} = (a, b)(-b^{-1}a, b^{-1}) = (a + b(-b^{-1}a), bb^{-1}) = (0, 1).\]
Finally, for (iii),

\[ x^{1/2}x^{1/2} = \left( \frac{a}{1 + b^{q+1}x^{1/2}}, b^{q+1}x^{1/2} \right) \left( \frac{a}{1 + b^{q+1}x^{1/2}}, b^{q+1}x^{1/2} \right) \]

\[ = \left( \frac{a}{1 + b^{q+1}x^{1/2}} + b^{q+1}x^{1/2}, b^{q+1}x^{1/2} \right) \]

\[ = \left( \frac{a(1 + b^{q+1})}{1 + b^{q+1}x^{1/2}}, b^{q+1}x^{1/2} \right) \]

\[ = (a, b). \]

Using these three facts, we now compute \( x \circ y = xy[y,x]^{1/2} \).

**Lemma 2.6.2.** Let \( x, y \in G \), with \( x = (a, b), y = (c, d) \). Then \( x \circ y = (1/2)[(1 + d)a + (1 + b)c], bd). \)

**Proof.** We compute

\[ x \circ y = xy[y,x]^{1/2} \]

\[ = (a + bc, bd)[(-d^{-1}c + d^{-1}(-b^{-1}a), d^{-1}b^{-1}(c + da, db)]^{1/2} \]

\[ = (a + bc, bd)[-d^{-1}c + d^{-1}(-b^{-1}a) + d^{-1}b^{-1}(c + da), d^{-1}b^{-1}db]^{1/2} \]

\[ = (a + bc, bd)[-d^{-1}c + d^{-1}b^{-1}a + d^{-1}b^{-1}c + b^{-1}a, 1]^{1/2} \]

\[ = (a + bc, bd)[-d^{-1}c + d^{-1}b^{-1}a + d^{-1}b^{-1}c + b^{-1}a, 1]^{2} \]

\[ = (a + bc + bd[-d^{-1}c + d^{-1}b^{-1}a + d^{-1}b^{-1}c + b^{-1}a, bd) \]

\[ = ((1/2)[(1 + d)a + (1 + b)c], bd). \]
To simplify following proofs, we have the following:

**Proposition 2.6.3.** Let \( x \in (G, \circ) \) with \( x = (a, b) \). Define \( \phi : G \to G \) with \( x \phi = ((b - 1)\alpha + a\beta, b) \) where \( \alpha, \beta \in \text{Aut}(G) \). Then \( \phi \in \text{Aut}(G) \).

**Proof.** Let \( x = (a, b), y = (c, d) \). Then we have

\[
(x \circ y)\phi = ((bd - 1)\alpha + ((1/2) [ (1 + d)a + (1 + b)c ] )\beta, bd).
\]

On the other hand

\[
\begin{align*}
x \phi \circ y \phi &= ((b - 1)\alpha + a\beta, b) \circ ((d - 1)\alpha + c\beta, d) \\
&= ((1/2) [ (1 + d)(b - 1)\alpha + a\beta ] + (1 + b)(d - 1)\alpha + c\beta ] , bd) \\
&= ((1/2) [ (2bd - 1)\alpha + [(1 + d)a + (1 + b)c]\beta ] , bd) \\
&= ((bd - 1)\alpha + ((1/2) [ (1 + d)a + (1 + b)c ] )\beta, bd).
\end{align*}
\]

Then we have the following.

**Theorem 2.6.4.** For all \( x, y \in G \), define \( x \circ y = xy[y, x]^{1/2} \). Then \( (G, \circ) \) is a commutative automorphic loop.

**Proof.** Let \( x, y, u, v \in (G, \circ) \) with \( x = (a, b), y = (c, d), u = (m, n), \) and \( v = (k, l) \). Note

\[
x \backslash y = \left( \frac{2c - (1 + b^{-1}d)a}{1 + b}, b^{-1}d \right).
\]
We need only to show \((u \circ v)L_{x,y} = uL_{x,y} \circ vL_{x,y}\), since we have shown \((G, \circ)\) is a commutative loop. Thus we compute

\[
uL_{x,y} = (y \circ x)(y \circ (x \circ u))
\]

\[
= \left(\frac{1}{2}[(1+b)c + (1+d)a], db\right)\left(\{(c, d) \circ ((1/2)[1+n]a + (1+b)m], bn\}\right)
\]

\[
= \left(\frac{1}{2}[(1+b)c + (1+d)a], db\right)\left(\{(1/2)[1+bn]c + (1+d)((1/2)[1+n]a + (1+b)m)], dbn\}\right)
\]

\[
= \left((1+bn)c + (1+d)((1/2)[1+n]a + (1+b)m] - (1+n)((1/2)[1+bn]c + (1+d)a], n)\right)
\]

\[
= \left((1+bn)c + (1+d)((1/2)[1+n]a + (1+b)m] - (1+n)((1/2)[1+bn]c + (1+d)a], n)\right)
\]

\[
= \left((1+bn)c + (1+d)((1/2)[1+n]a + (1+b)m] - (1+n)((1/2)[1+bn]c + (1+d)a], n)\right)
\]

\[
= \left((1+bn)c + (1+d)((1/2)[1+n]a + (1+b)m] - (1+n)((1/2)[1+bn]c + (1+d)a], n)\right)
\]

We let \(\alpha = bc - c\) and \(\beta = (b + d + bd + 1)\) and thus, by Proposition 2.6.3, \(L_{x,y}\) is an automorphism and hence, \((u \circ v)L_{x,y} = uL_{x,y} \circ vL_{x,y}\).

\[\square\]
Chapter 3

Semiautomorphic Inverse Property Loops

In this chapter, we focus a class of loops generalizing both Moufang loops and Steiner loops. Recall in a flexible loop $Q$, a permutation $\theta : Q \rightarrow Q$ is a semiautomorphism if

$$(xyx)\theta = x\theta \cdot y\theta \cdot x\theta,$$

for all $x, y \in Q$. Every inner mapping $\theta$ of a Moufang loop and a Steiner loop is a semiautomorphism.

3.1 Semiautomorphic inverse property loops

Definition 3.1.1. A loop $Q$ is said to be a semiautomorphic, inverse property loop (or just semiautomorphic IP loop) if

1. $Q$ is flexible;
2. \( Q \) has the inverse property;

3. Every inner mapping is a semiautomorphism, that is, for each \( \theta \in \text{Inn}(Q) \),
\[ x\theta \cdot y\theta \cdot x\theta = (x \cdot y \cdot x)\theta \text{ for all } x, y \in Q. \]

**Remark 3.1.2.** We could have dispensed with flexibility as part of the definition and simply fixed a convention for what a semiautomorphism is, such as \( x\theta \cdot (y\theta \cdot x\theta) = (x \cdot (y \cdot x))\theta\). However, it is easy to show that flexibility is then a consequence.

If \( \theta \) is a semiautomorphism of a flexible loop \( Q \), then for all \( x \in Q \), \( x\theta = (xx^{-1})\theta = x\theta \cdot x^{-1} \cdot x\theta \), and cancelling gives \( 1 = x\theta \cdot x^{-1}\theta \). Thus recalling the inversion map \( J: Q \rightarrow Q \) by \( xJ = x^{-1} \), we have \( \theta^J = \theta \) for any semiautomorphism \( \theta \).

It follows that any semiautomorphic IP loop is an example of a variety of loops which have already appeared in the literature called “J-loops” or “RIF loops” (RIF = Respects Inverses and Flexible). J-loops were introduced in [23] and RIF loops were introduced in [32]. Commutative RIF loops were studied in [35]. Recalling that a loop is diassociative if any subloop generated by at most two elements is associative, we have the following, which follows from the main result of [32].

**Proposition 3.1.3.** [32]. Every semiautomorphic IP loop is diassociative.

**Remark 3.1.4.** Throughout, we will make explicit use of diassociativity for simplifications, without reference.

Our first main result, proved at the end of this section, is the converse of our observation that every semiautomorphic IP loop is a RIF loop (eschewing the somewhat cryptic “RIF” terminology).

**Theorem 3.1.5.** Let \( Q \) be a loop. The following are equivalent.
1. \(Q\) is a semiautomorphic IP loop;

2. \(Q\) is a flexible IP loop such that \(\theta^J = \theta\) for all \(\theta \in \text{Inn}(Q)\).

**Lemma 3.1.6.** [23, 32]. Let \(Q\) be an IP loop. Then the following are equivalent:

(3.1.6.1) For all \(\theta \in \text{Inn}(Q)\), \(x^{-1}\theta = (x\theta)^{-1}\).

(3.1.6.2) \(Q\) is flexible and \(R_{xy} = L_{x^{-1}y^{-1}}\) for all \(x, y \in Q\).

(3.1.6.3) \(R_{xy}L_{xy} = L_{x}L_{x}R_{x}R_{y}\) for all \(x, y \in Q\).

(3.1.6.4) \(L_{xy}R_{xy} = R_{x}R_{y}L_{x}L_{y}\) for all \(x, y \in Q\).

By flexibility, the left hand sides of (3.1.6.3) and (3.1.6.4) are equal and thus we can equate (3.1.6.3) with either side of (3.1.6.4). For convenience, define

\[P_x = L_xR_x = R_xL_x\]

by flexibility. Then in an IP loop conditions (3.1.6.3) and (3.1.6.4) can be written as

\[L_xP_yR_x = P_{yx}, \quad \text{(RIF1)}\]
\[R_xP_yL_x = P_{xy}. \quad \text{(RIF2)}\]

We will use the RIF acronym as an equation label for historical reference. We also use the ARIF condition,

\[R_xR_{yxy} = R_{xy}R_y, \quad L_xL_{yxy} = L_{xy}L_y. \quad \text{(ARIF)}\]
which hold in any loop satisfying the conditions of Lemma 3.1.6; see [32].

**Theorem 3.1.7.** Let $Q$ be an IP loop satisfying (RIF1) and (RIF2). Then every inner mapping is a semiautomorphism.

**Proof.** By (3.1.6.2), it is enough to show that each $T_x$ and each $R_{x,z}$ is a semiautomorphism. Note that an inner mapping $\theta$ is a semiautomorphism if and only if $P_x \theta = \theta P_x$ for all $x \in Q$. First, $1 = 1T_x = 1R_{x,y}$ by definition. Thus we compute

$$P_yT_x = P_yR_xL_{x^{-1}} \quad \text{(RIF1)} = L_{x^{-1}}P_yL_{x^{-1}} \quad \text{(RIF2)} = L_{x^{-1}}R_xP_{x^{-1}y} = T_xP_yT_x.$$ 

For $R_{x,y}$, we compute

$$P_yR_{x,z} = P_yR_xR_zR_{(xz)}^{-1} \quad \text{(RIF1)} = L_{x^{-1}}P_yR_zR_{(xz)}^{-1} \quad \text{(RIF1)} = L_{x^{-1}}L_{z^{-1}}P_{yxz}R_{yz(z)}^{-1} \quad \text{(RIF1)} = L_{x^{-1}}L_{z^{-1}}L_{xyz}P_{yxz}R_{xz}^{-1} \quad \text{(RIF1)} = L_{x^{-1}}P_yR_{z} = R_{x,z}P_yR_{xz}.$$ 

Hence, we have shown that semiautomorphic IP loops coincide with the variety formerly known as RIF loops.

**Proof of Theorem 3.1.5.** This follows immediately from Theorem 3.1.7 and the earlier observation that semiautomorphisms preserve inverses. 

\[\square\]
3.2 Commutant of a Semiautomorphic loop

In general, the commutant of a loop is not a subloop, although it is known to be so in certain cases. In a Moufang loop $Q$, it is noted in [8] that $C(Q)$ is a subloop and an explicit proof is given in [42]. In this section we will prove the same result for semiautomorphic IP loops, proved towards the end of the section.

**Theorem 3.2.1.** The commutant of a semiautomorphic IP loop is a subloop.

The set of Moufang elements, are

$$M(Q) = \{ a \in Q \mid a(xy \cdot a) = ax \cdot ya, a(x \cdot ay) = (ax \cdot a)y, (ya \cdot x)a = y(a \cdot xa), \forall x, y \in Q \}.$$

The set $M(Q)$ of Moufang elements is also a subloop of any loop [43]. Toward showing $C(Q)$ is a subloop, we also show that for any $a \in C(Q)$, $a^2$ is a Moufang element.

**Theorem 3.2.2.** Let $Q$ be a semiautomorphic IP loop and let $a \in C(Q)$. Then $a^2$ is a Moufang element.

This immediately gives us that for each $a \in C(Q)$, $a^6 \in Z(Q)$, where $Z(Q)$ denotes the center of $Q$ (Corollary 3.2.14). This simultaneously generalizes two results: that in a Moufang loop, the cube of any commutant element is central [8], and that in a commutative semiautomorphic IP loop, the sixth power of any element is central [35].

We note that in an IP loop $Q$, to verify that a subset $S$ is a subloop, it is sufficient to check that $S$ is closed under multiplication and taking inverses. The proof will occupy most of this section and will require some technical lemmas. We note that
in a semiautomorphic IP loop \(Q\), each \(\theta \in \text{Inn}(Q)\) preserves powers, that is, \(x^n\theta = (x\theta)^n\) for all \(x \in Q, n \in \mathbb{Z}\). We will use this without comment in what follows.

**Lemma 3.2.3.** [35]. In a semiautomorphic IP loop \(Q\), \(a \in M(Q)\) if and only if \((yx \cdot a)x = y \cdot xax\) for all \(x, y \in Q\).

**Lemma 3.2.4.** Let \(Q\) be a dissociative loop and \(a \in C(Q)\). Then \(\langle a \rangle \subseteq C(Q)\).

*Proof.* We simply note \(a^n x = xL_a^n = xL_a^n = xR_a^n = xR_a^n = xa^n\).

**Lemma 3.2.5.** Let \(Q\) be a diassociative loop. For all \(a \in C(Q), x \in Q\) and all \(n \in \mathbb{Z}\), \((xa)^n = x^n a^n\).

*Proof.* This follows easily from Lemma 3.2.4 and an induction argument.

**Lemma 3.2.6.** Let \(Q\) be a semiautomorphic IP loop and let \(a \in C(Q)\). For all \(x \in Q\)

\[
P_a L_x R_a L_x^{-1} = L_x R_a L_x^{-1} P_a. \tag{3.2.6.1}
\]

*Proof.* We have \(P_a L_x R_a L_x^{-1} = P_a \theta R_a\) where \(\theta = L_x R_a L_x^{-1} R_a^{-1} \in \text{Inn}(Q)\). Since \(\theta\) is a semiautomorphism, \(P_a \theta = \theta P_a \theta\). We have \(a \theta = a L_a R_a L_a^{-1} R_a^{-1} = a\) by diassociativity, and so \(P_a L_x R_a L_x^{-1} = L_x R_a L_x^{-1} R_a^{-1} P_a R_a = L_x R_a L_x^{-1} P_a\), as claimed.

**Lemma 3.2.7.** Let \(Q\) be a semiautomorphic IP loop and let \(a \in C(Q)\). For all \(x \in Q\)

\[
R_{ax}^2 = R_a R_{ax}^2 R_a \quad L_{ax}^2 = L_a L_{ax}^2 L_a. \tag{3.2.7.1}
\]
Proof. Using diassociativity, we have
\[ x = (x \cdot ay)(ya)^{-1} = (x \cdot ay)^2[(x \cdot ay)^{-1}(ya)^{-1}] = (x \cdot ay)^2[ya \cdot x \cdot ay]^{-1}, \]
and so
\[ x = (x \cdot ay)^2R^{-1}_{(ya \cdot x \cdot ay)}. \]
(3.2.7.2)

Our intermediate goal is to prove
\[ [(xy)^2]L_{x^{-1}}L_{aL_{ax}} = (a \cdot xy)^2 \]
(3.2.7.3)

We have
\[ [(xy)^2]L_{x^{-1}}L_{aL_{ax}} = [(xy)^2]\theta L_{a^2} = a^2 \cdot [(xy)^2]\theta \]
where \( \theta = L_{x^{-1}}L_{aL_{ax}}L_{a^{-2}} \in \text{Inn}(Q) \). Since inner mappings preserve powers, we then have
\[ [(xy)^2]L_{x^{-1}}L_{aL_{ax}} = a^2 \cdot [(xy)\theta]^2 = [a \cdot (xy)\theta]^2. \]

Now
\[ a \cdot (xy)\theta = (ax \cdot a(x^{-1} \cdot xy))L_{a^{-2}L_{a}} = (ax)R_{ay}P_{a^{-1}}L_{a} \]
\[ \overset{\text{(RIF1)}}{=} P_{y}L_{ay}^{-1}L_{a} \]
\[ = [(ay)^{-1}]R_{(ax)}P_{a}L_{a} \]
\[ = (x \cdot ay)R_{(ay \cdot x \cdot ay)}^{-1}R_{(ax)}P_{a}L_{a} = (x \cdot ay)\varphi, \]
where \( \varphi = R_{x \cdot ay}^{-1}R_{(ax)}P_{y}L_{a} \) and where the fifth equality follows from diassociativity.

Thus
\[ [(xy)^2]L_{x^{-1}}L_{aL_{ax}} = [(x \cdot ay)\varphi]^2. \]
Since
\[ xP_{ay} \overset{(\text{RIF1})}{=} (xa)P_yL_a = a \cdot (ax)P_y, \]
we see that \( \varphi = R_{ax}^{-1}P_yR_{ax}P_yL_a \) is an inner mapping. So putting our calculations together, we have

\[
[(xy)^2]L_{x^{-1}}L_aL_{ax} = [(x \cdot ay)^2] \overset{3.2.7.2}{=} xR_{(ax)}P_yL_a = aR_{x}P_yL_a L_a = a \cdot x^{-1}y \cdot a \cdot xy
\]

= \((a \cdot xy)^2\).

This establishes (3.2.7.3). Now in (3.2.7.3), replace \( y \) with \( x^{-1}y \) and rearrange to get

\[(ax)^{-1} \cdot (ay)^2 = a \cdot x^{-1}y^2.\]

Then replace \( x \) with \((ax)^{-1}\) and simplify to get

\[x \cdot (ay)^2 = a(ax \cdot y^2),\]

that is, \( xR_{(ay)^2} = xR_{a}R_{y^2}R_{a} \). This establishes half of the desired result, and the other half follows by a dual argument.

\[\square\]

**Lemma 3.2.8.** Let \( Q \) be a semiautomatic IP loop and let \( a \in C(Q) \). For all \( x \in Q \)

\[R_xR_{ax^{-1}}^{-1}R_a = R_aR_xR_{a^2x}^{-1}. \tag{3.2.8.1}\]
Proof. Since $x = ax \cdot (a^2 x)^{-1} \cdot ax$, we have

$$R_x R_{a^2 x}^{-1} R_a = R_{ax \cdot (a^2 x)^{-1} \cdot ax} (a) R_{a^2 x}^{-1} \cdot ax \cdot R_a \overset{\text{(ARIF)}}{=} R_{ax \cdot (a^2 x)^{-1} \cdot ax \cdot (a^2 x)^{-1}} R_a.$$ 

Now $(a^2 x)^{-1} \cdot ax \cdot (a^2 x)^{-1} = a^{-1} \cdot (ax)^{-1} \cdot a^{-1}$ and $R_{ax} = R_{ax} R_{(ax)^{-1}}$, and so by the above,

$$R_x R_{a^2 x}^{-1} R_a = R_{ax} R_{ax}^{-1} a^{-1} \cdot R_{ax} \cdot R_{ax}^{-1} \cdot R_{ax} R_{ax}^{-1} R_a \overset{\text{(ARIF)}}{=} R_{ax} R_{ax}^{-1} a^{-1} \cdot R_{ax} R_{ax}^{-1} R_a R_{ax}.$$ 

We have $R_{ax}^2 = R_{ax} R_{ax} R_a$ by Lemma 3.2.7 and $(ax)^{-1} \cdot a^{-1} \cdot (ax)^{-1} = (a^2 x)^{-1} \cdot a \cdot (a^2 x)^{-1}$, and so

$$R_x R_{a^2 x}^{-1} R_a = R_a R_{x^2} R_{a} R_{a^2 x}^{-1} a^{-1} \cdot R_{a^2 x}^{-1} R_{a} R_{a^2 x}^{-1} R_a \overset{\text{(ARIF)}}{=} R_a R_x R_{a^2 x}^{-1} a \cdot R_{a^2 x}^{-1} R_a \overset{\text{(ARIF)}}{=} R_a R_x R_{a^2 x}^{-1} R_{a^2 x}^{-1} R_a,$$

as claimed. \hfill \Box

Lemma 3.2.9. Let $Q$ be a semiautomorphic IP loop and let $a \in C(Q)$. For all $x \in Q$

$$(xy)^{-1} \cdot ax = ax \cdot (yx)^{-1}. \quad (3.2.9.1)$$

Proof. By diassociativity, $ax = (xy \cdot y^{-1}) a = (xy \cdot (a \cdot (a^2 y)^{-1} \cdot a) \cdot a$, and so we have

$$(xy)^{-1} \cdot ax = (xy)^{-1} \cdot (xy \cdot (a \cdot (a^2 y)^{-1} \cdot a)) a = [(a^2 y)^{-1}]_{P_a} L_{xy} R_a L_{(xy)^{-1}}$$

$$\overset{(3.2.6.1)}{=} [(a^2 y)^{-1} L_{xy} R_a L_{(xy)^{-1}} P_a = x R_{a^2 y}^{-1} R_a L_{(xy)^{-1}} P_a$$

48
\[(3.2.8.1) \quad xR_a R_y R_{(a^2 y)^{-1} L_{(xy)^{-1}}} R_a.\]

Now
\[
(xa \cdot y)(a^2 y)^{-1} = (a^2 y)^{-1} P_{xa} R_{(xa \cdot y)^{-1}} \overset{\text{RIF2}}{=} (a^2 y)^{-1} L_y P_{xa} R_{(xa \cdot y)^{-1}}
\]
\[
= (x^2) R_y R_{(xa \cdot y)^{-1}} = (x^2 y) R_{(xa \cdot y)^{-1}},
\]
using diassociativity in the third equality. Combining this with the calculation above, we have
\[
(xy)^{-1} \cdot ax = (x^2 y) R_{(xa \cdot y)^{-1}} L_{(xy)^{-1}} P_a = [(xa \cdot y)^{-1}] L_y x^2 y L_{(xy)^{-1}} P_a.
\]
Since \(x^2 y = xy \cdot y^{-1} \cdot xy\), we get
\[
(xy)^{-1} \cdot ax = [(xa \cdot y)^{-1}] L_y L_{y^{-1}} L_{xy \cdot y^{-1}} L_{(xy)^{-1}} L_{(xy)^{-1}} P_a
\]
\[
= [(xa \cdot y)^{-1}] L_y L_{y^{-1}} L_{xy \cdot y^{-1}} L_{(xy)^{-1}} P_a
\]
\[
= [(xa \cdot y)^{-1}] L_y L_{y^{-1}} L_{xy \cdot y^{-1}} P_a.
\]
Now \([(xa \cdot y)^{-1}] L_y = (xa)^{-1}\) and \(y^{-1} \cdot xy \cdot y^{-1} = y^{-1} x\), and so
\[
(xy)^{-1} \cdot ax = [(xa)^{-1}] L_{y^{-1}} P_a = (y^{-1} x) R_{(xa)^{-1} P_a L_{(ax)^{-1}}} L_{ax}
\]
\[
= (y^{-1} x) P_{(ax)^{-1} L_{ax}} = (x^{-1} y^{-1}) L_{ax}
\]
\[
= ax \cdot (yx)^{-1},
\]
using \((xa)^{-1} \cdot a = x^{-1}\) in the second equality. This completes the proof. \(\square\)
Lemma 3.2.10. Let $Q$ be a semiautomorphic IP loop and let $a \in C(Q)$. For all $x \in Q$

$$T_{ax} = T_x \quad (3.2.10.1)$$

Proof. Invert both sides of (3.2.9.1) to get

$$(ax)^{-1} \cdot xy = yx \cdot (ax)^{-1}$$

which is

$$L_x L_{ax}^{-1} = R_x R_{ax}^{-1}.$$ 

Rearranging gives

$$L_{ax}^{-1} R_{ax} = L_x^{-1} R_x,$$

which establishes the claim. \qed

We are now ready to prove the two main results of this section.

Proof of Theorem 3.2.2. Let $a \in C(Q)$. Then for all $x \in C(Q)$,

$$R_x R_{a^2} R_x = R_x P_a R_x \overset{(RIF1)}{=} R_x L_x^{-1} P_{ax} = T_x P_{ax} = T_{ax} P_{ax} = R_{ax} L_{ax}^{-1} R_{ax} L_{ax} = R_{ax} L_{ax}^{-1} L_{ax} R_{ax} = R_{ax} R_{ax} = R_{ax}^2 = R_{ax^2} = R_{ax^2 x},$$

where the fourth equality follows from Lemma 3.2.10. Hence,

$$(yx \cdot a^2) x = y R_x R_{a^2} R_x = y R_{ax^2} = y (x \cdot a^2 \cdot x).$$

50
By Lemma 3.2.3, we have the desired result. 

Proof of Theorem 3.2.1. Let $a, b \in C(Q)$. Then, for all $x, y \in Q$,

$$ab \cdot x \cdot ab \overset{(RIF2)}{=} a(b \cdot xa \cdot b) = (xa \cdot b) \cdot a = \underbrace{(xa \cdot b^2)} \cdot a$$

$$= x \cdot ab^2 a = x \cdot (ab)^2 = (x \cdot ab) \cdot ab,$$

where the fourth equality follows from the fact that $b^2$ is a Moufang element, Theorem 3.2.2. Hence, cancelling $ab$ on the right gives $ab \cdot x = x \cdot ab$. 

Lemma 3.2.11. [8]. Let $Q$ be an IP loop. Then for every $x \in M(Q) \cap C(Q)$, $x^3 \in Z(Q)$.

Thus, we have the following,

Corollary 3.2.12. Let $Q$ be a semiautomorphic IP loop. If $a \in C(Q)$, then $a^6 \in Z(Q)$.

Proof. This immediately follows from Theorem 3.2.2 and Lemma 3.2.11.

An element $a$ of a loop $Q$ is a $C$-element if it satisfies the following equation for all $x, y \in Q$.

$$x(a \cdot ay) = (xa \cdot a)y \quad (C_0)$$

We denote $C_0(Q)$ be the set of all $C$-elements in a loop $Q$.

Lemma 3.2.13. [11]. In an IP loop $Q$, $a \in C_0(Q)$ if and only if $a^2 \in N(Q)$.

Hence we have the following,

Corollary 3.2.14. Let $Q$ be a semiautomorphic IP loop. If $a \in C(Q)$, then $a^3$ is a $C$-element.

Proof. This follows immediately from Theorem 3.2.12 and Lemma 3.2.13.
3.3 Constructing semiautomorphic IP loops

We now discuss two constructions for semiautomorphic IP loops. There is a well-known doubling construction of Chein which builds nonassociative Moufang loops from nonabelian groups. The construction itself makes sense even when one starts with a loop instead of a group. It turns out that if one applies the construction to a semiautomorphic IP loop, the result is another semiautomorphic IP loop (Theorem 3.3.5). In particular, this allows us to construct nonMoufang, nonSteiner, semiautomorphic IP loops by starting with nonassociative Moufang loops.

The following will be used without comment.

**Lemma 3.3.1.** [34]. Let $Q$ be an IP loop and $*: Q \to Q$ a map such that $gg^* \in Z(Q)$ for every $g \in Q$. Then $g^*g = gg^* \in Z(Q)$ for every $g \in Q$.

**Proof.** Since $Q$ in an IP loop,

$$g^*g = (g^{-1} \cdot gg^*)g = (gg^* \cdot g^{-1})g = gg^*.$$

**Theorem 3.3.2.** Let $Q$ be an IP Loop and $*$ be an involutory antiautomorphism. Then $\forall x, y \in Q$,

$$x \cdot yy^* = xy \cdot y^*, \quad (3.3.2.1)$$

$$xx^* \cdot y = x \cdot x^* y, \quad (3.3.2.2)$$

$$x(yy^*) \cdot x^* = xy \cdot y^* x^*. \quad (3.3.2.3)$$
Proof. For (3.3.2.1), simply note that

\[ x \cdot yy^* = (xy \cdot y^{-1}) \cdot yy^* = xy \cdot (y^{-1} \cdot yy^*) = xy \cdot y^*. \]

Similarly for (3.3.2.2), since \( xx^* \in Z(Q) \), we have \( x^{-1}(xx^* \cdot y) = (x^{-1} \cdot xx^*)y = x^*y. \) Multiply by \( x \) on the left to get \( xx^* \cdot y = x \cdot x^*y. \)

For (3.3.2.3), we see \( yy^* = yy^* \cdot x^{-1}x = x^{-1}(yy^* \cdot x) (3.3.2.2) x^{-1} \cdot y(y^*x). \) Now replace \( x \) and \( y \) with \( y^{-1}x \) and \( y^* \) and get \( x^{-1}y^* \cdot yx = yy^*. \) Now,

\[ x^*y \cdot z = (x^{-1} \cdot xx^*)y \cdot z = xx^*(x^{-1}y \cdot z) (3.3.2.2) x \cdot x^*(x^{-1}y \cdot z). \]

Now, we substitute \( z = (yx) \) and \( y = y^* \) getting

\[ x^*y^* \cdot yx = x \cdot x^*(x^{-1}y^* \cdot yx) = xx^*(x^{-1}y \cdot z) (3.3.2.2) y(xx^*) \cdot y^*. \]

Since \( x^*y^* \cdot yx = yx \cdot x^*y^* \), we have \( yx \cdot x^*y^* = y(xx^*) \cdot y^*. \) □

3.3.1 Generalizing Chein’s Construction

We first need a technical lemma.

Lemma 3.3.3. Let \( Q \) be a semiautomorphic IP loop and let \( * \) be a semiautomorphism of \( Q \) such that

\[ (g^*)^* = g, \]  

\[ g^*h \cdot (k \cdot g^*h)^* = (g \cdot h^*k)^*g \cdot h^*. \]  

53
Then for all \( g, h \in Q \),

\[
g(hg)^* = (g^*h)^*g^*, \tag{3.3.3.2.i}
\]
\[
((gh)^*)^* = (g^*h^*)^*g^*, \tag{3.3.3.2.ii}
\]
\[
(g(hg)^*)^* = g^*(h^*g^*)^*. \tag{3.3.3.2.iii}
\]

**Proof.** Recall that \((x^{-1})^* = (x^*)^{-1}\) for all \( x \in Q \) since \(*\) is a semiautomorphism.

For (3.3.3.2.i), simply let \( g = 1 \) in (3.3.3.2). For (3.3.3.2.ii), we see

\[
g^* = ((g^*h)^{-1}((g^*h)^* \cdot g^*) = ((g^*h)^{-1})^*(g(hg)^*) = (h^{-1}(g^*h)^{-1}^*)(g(hg)^*).
\]

Replace \( h \) with \( h^{-1} \) and then interchange \( g \) and \( h \) gives \( h = (gh^{-1})^*(h^*(g^{-1}h^*)^*) \).

Applying this to (3.3.3.2), we get

\[
(hg)^* = (h(gh^{-1} \cdot h))^* = (h^* \cdot (gh^{-1})^*) \cdot h^*
\]

Using this and (3.3.3.2.i), we have

\[
(g(hg)^*)^* \overset{(3.3.3.2.i)}{=} ((g^*h)^*g^*)^* = g^*(((g^{-1})^*((g^*h)^*)^*g^*)^* = g^*(((g^{-1})^*g^*h)^*)^* = (h^*g^*)^* \overset{(3.3.3.2.i)}{=} (gh^*)^*g.
\]

54
Therefore, we have \((g^*h^*)^*g^* = (g^*(hg^*)^*)^* = ((gh)^*)^*\). Lastly, (3.3.3.2.iii) follows from (3.3.3.2.ii) and the previously stated fact that semiautomorphisms respect inverses. We use these results without comment in what follows.

**Lemma 3.3.4.** Let \(Q\) be a semiautomorphic IP loop, let \(g_0 \in Z(Q)\) be fixed and let \(*\) be a semiautomorphism of \(Q\) such that, for all \(g, h, k \in Q\)

\[
(g^*)^* = g, \tag{3.3.4.1}
\]
\[
(gg_0)^* = g^*g_0, \tag{3.3.4.2}
\]
\[
g^*h \cdot (k \cdot g^*h)^* = (g \cdot h^*k)^*g \cdot h^*. \tag{3.3.4.3}
\]

For an indeterminate \(t\), define multiplication \(\circ\) on \(Q \cup Qt\) by

\[
g \circ h = gh, \quad g \circ (ht) = (g^*h^*)^*t, \quad gt \circ h = (gh^*)t, \quad gt \circ ht = g_0(g^*h)^*,
\]

where \(g, h \in Q\). Then \((Q \cup Qt, \circ)\) is a semiautomorphic IP loop.

**Proof.** To show \((Q \cup Qt, \circ)\) satisfies (RIF1), eight cases arise, depending on whether our elements are from \(Q\) or \(Qt\). Note that by Lemma 3.3.1, any time we see an expression \(xx^* = x^*x\) for any \(x \in Q\), we can commute and associate this term to any place in our equation. Similarly for \(g_0\), however here we will always put \(g_0\) to the far left of our equations. We will do this without reference. Let \(x, y, z \in (Q \cup Qt, \circ)\).

**Case 1.** \(x, y, z \in Q\). Then we are finished.

**Case 2.** \(x, y \in Q\) and \(z \in Qt\), so let \(x = g, y = h, z = kt\) for some \(g, h, k \in Q\). Thus

\[
(x \circ y) \circ (z \circ (x \circ y)) = (g \circ h) \circ (kt \circ (g \circ h))
\]
\[
= gh \circ (k \cdot (gh)^*)t
\]
\[(3.3.3.2.1)\]
\[
\begin{align*}
&= [(gh)^*(k \cdot (gh)^*)]^*t \\
&\overset{(3.3.3.2.1)}{=} [gh \cdot (k^* \cdot gh)^*]t \\
&\overset{(3.3.4.3)}{=} [(g^* \cdot h^* k^*)^* g^* \cdot h^*]t \\
&= ((g^* \cdot h^* k^*)^* g^*)t \circ h \\
&= ((g^* \cdot h^* k^*)^* t \circ g) \circ h \\
&= ((g \circ (h^* k^*)^* t) \circ g) \circ h \\
&= ((g \circ (h \circ k t)) \circ g) \circ h \\
&= ((x \circ (y \circ z)) \circ x) \circ y.
\end{align*}
\]

**Case 3.** \(x, z \in Q\) and \(y \in Qt\), so let \(x = g, y = ht, z = k\) for some \(g, h, k \in Q\). Thus

\[
(x \circ y) \circ (z \circ (x \circ y)) = (g \circ ht) \circ (k \circ (g \circ ht))
\]
\[
= (g^* h^*)^* t \circ (k \circ (g^* h^*)^* t)
\]
\[
= (g^* h^*)^* t \circ (k \cdot g^* h^*)t
\]
\[
= g_0[g^* h^* \cdot (k \cdot g^* h^*)^*]^*
\]
\[
\overset{(3.3.4.3)}{=} g_0[(g \cdot h k^*)^* g^* \cdot h]^*
\]
\[
\overset{(3.3.3.2.ii)}{=} g_0[(g^* (h k^*)^* \cdot g^*)^* \cdot h]^*
\]
\[
= (((g^* (h k^*)^*)^*) \cdot g^*)t \circ ht
\]
\[
= (g^* (h k^*)^* t \circ g) \circ ht
\]
\[
= ((g \circ (h k^*)^* t) \circ g) \circ ht
\]
\[
= ((g \circ (ht \circ k)) g \circ) \circ ht
\]
\[
= ((x \circ (y \circ z)) \circ x) \circ y.
\]
Case 4. \( y, z \in Q \) and \( x \in Qt \), so let \( x = gt, y = h, z = k \) for some \( g, h, k \in Q \). Thus

\[
(x \circ y) \circ (z \circ (x \circ y)) = (gt \circ h) \circ (k \circ (gt \circ h))
\]
\[
= (gh^*)t \circ (k \circ (gh^*)t)
\]
\[
= (gh^*)t \circ (k^* \cdot (gh^*)^*)^*t
\]
\[
= g_0 [([gh^*] \cdot (k^* \cdot (gh^*)^*)]^*)^*\]
\[
= g_0 [([gh^*] \cdot (k^* \cdot (gh^*)^*)])^*\]
\[
= g_0 [((g \cdot (hk^*)) \cdot g)^h]\]
\[
= ((g \cdot (hk^*))t \circ gt) \circ h
\]
\[
= ((gt \circ (h \circ k)) \circ gt) \circ h
\]
\[
= ((x \circ (y \circ z)) \circ x) \circ y.
\]

Case 5. \( z \in Q \) and \( x, y \in Qt \), so let \( x = gt, y = ht, z = k \) for some \( g, h, k \in Q \). Thus

\[
(x \circ y) \circ (z \circ (x \circ y)) = (gt \circ ht) \circ (k \circ (gt \circ ht))
\]
\[
= g_0 g_0 ((g^*h)^* \circ (k \cdot (g^*h)^*))
\]
\[
= g_0 g_0 (g^*h \cdot (k^* \cdot (g^*h))^*)
\]
\[
= g_0 (((g^* \cdot hk^*)^*t \circ ht)
\]
\[
= g_0 (((g^* \cdot hk^*)^* \circ gt) \circ ht)
\]
\[
= (((gt \circ hk^*)t) \circ gt) \circ ht
\]
\[
= (((gt \circ (ht \circ k)) \circ gt) \circ ht
\]
\[
= ((x \circ (y \circ z)) \circ x) \circ y.
\]
Case 6. $x, z \in Q$ and $y \in Qt$, so let $x = gt, y = h, z = kt$ for some $g, h, k \in Q$. Thus

$$(x \circ y) \circ (z \circ (x \circ y)) = (gt \circ h) \circ (kt \circ (gt \circ h))$$

$$= (gh^*)t \circ (kt \circ (gh^*)t)$$

$$= g_0((gh^*)t \circ (k^* \cdot gh^*)^*)$$

$$= g_0((gh^*) \cdot (k^* \cdot gh^*))t$$

(RIF1) $$= g_0((g \cdot h^*k^*)g \cdot h^*)t$$

(3.3.3.2.i) $$= g_0(((g^* \cdot (h^*k^*)^*)g^*)^* \cdot h^*)t$$

$$= g_0(((g^* \cdot (h^*k^*)^*)^*t \circ h)$$

$$= g_0(((g^* \cdot (h^*k^*)^*)^* \circ gt) \circ h)$$

$$= ((gt \circ (h^*k^*)^*t) \circ gt) \circ h$$

$$= ((gt \circ (h \circ kt)) \circ gt) \circ h$$

$$= ((x \circ (y \circ z)) \circ x) \circ y.$$ 

Case 7. $x \in Q$ and $y, z \in Qt$, so let $x = g, y = ht, z = kt$ for some $g, h, k \in Q$. Thus

$$(x \circ y) \circ (z \circ (x \circ y)) = (g \circ ht) \circ (kt \circ (g \circ ht))$$

$$= (g^*h^*)^*t \circ (kt \circ (g^*h^*)^*)$$

$$= g_0((g^*h^*)^*t \circ (k^* \cdot (g^*h^*)^*))$$

$$= g_0((g^*h^*)^* \cdot (k^* \cdot (g^*h^*)^*))t$$

(3.3.3.2.i) $$= g_0((g^*h^*)^* \cdot (k \cdot (g^*h^*)))^*t$$

(RIF1) $$= g_0((g^*h^*k^*)g^* \cdot h^*)^*t$$

(3.3.3.2.i) $$= g_0((g(h^*k^*)^* \cdot g)^* \cdot h^*)^*t$$
\(= g_0((g \cdot (h^*k)^*)g \cdot ht)\)
\(= ((g \cdot (ht \circ kt)) \circ g) \cdot ht\)
\(= ((x \circ (y \circ z)) \circ x) \circ y.\)

**Case 8.** \(x, y, z \in Qt\), so let \(x = gt, y = ht, z = kt\) for some \(g, h, k \in Q\). Thus

\[(x \circ y) \circ (z \circ (x \circ y)) = (gt \circ ht) \circ (kt \circ (gt \circ ht))\]
\(= g_0 g_0((g^*h)^* \circ (kt \circ (g^*h)^*))\)
\(= g_0 g_0((g^*h)^* \circ (k \cdot (g^*h)^*)t)\)
\(= g_0 g_0((g^*h)^* \cdot (k \cdot (g^*h)^*))^* t\)
\(= g_0 g_0((g \cdot h^* k)^* g \cdot h^*)^* t\)
\(= g_0((g \cdot h^* k \circ g^* h)^* \circ ht)\)
\(= g_0((g \cdot h^* k \circ g^* h \circ h) \circ ht)\)
\(= ((gt \circ (ht \circ kt)) \circ gt) \circ ht\)
\(= ((x \circ (y \circ z)) \circ x) \circ y.\)

Now, to see \((Q \cup Qt, \circ)\) is an IP loop, suppose \(x \in Qt\) and let \(x = gt\) for some \(g \in Q\).

Then note

\[1 \circ x = 1 \circ gt = (1g^*)^* t = gt = x = gt = (g1^*)t = gt \circ 1 = x \circ 1.\]

Moreover, \(x^{-1} = (gt)^{-1} = (g_0^{-1} g^{-1})t\), where \(g^{-*} = (g^{-1})^* = (g^*)^{-1}\). For \(x^{-1} \circ (x \circ y) = y\), we have 4 cases:
Case 1. \(x, y \in Q\), so we are done.

Case 2. \(x \in Q\) and \(y \in Qt\), so let \(x = g, y = ht\) for some \(g, h \in Q\). Thus

\[
g^{-1} \circ (g \circ ht) = g^{-1} \circ (g^*h)^*t = (g^{-*}(g^*h))^{*}t = (h^*)^*t = ht.
\]

Case 3. \(x \in Qt\) and \(y \in Q\), so let \(x = gt, y = h\) for some \(g, h \in Q\). Thus

\[
(gt)^{-1} \circ (gt \circ h) = (g_0^{-1}g^{-*})t \circ (gh^*)t = g_0[(g_0^{-1}g^{-*}) \cdot gh^*]^{*}t
\]
\[
= g_0[g_0^{-1}(g^{-*}) \cdot gh^*]^* = g_0[g_0^{-1}g^{-1} \cdot gh^*]^*
\]
\[
= g_0(g_0^{-1}h^*)^* = g_0 \cdot g_0^{-1}(h^*)^* = h.
\]

Case 4. \(x \in Qt\) and \(y \in Qt\), so let \(x = gt, y = ht\) for some \(g, h \in Q\). Thus

\[
(gt)^{-1} \circ (gt \circ ht) = (g_0^{-1}g^{-*})t \circ (g_0(g^*h)^*) = [g_0^{-1}g^{-*} \cdot (g_0(g^*h)^*)]^*t
\]
\[
= [g_0^{-1}g^{-*} \cdot g_0((g^*h)^*)]^*t = [g_0^{-1}g^{-*} \cdot g_0(g^*h)]^*t
\]
\[
= (g^{-*} \cdot g^*h)t = ht.
\]

Finally, \((y \circ x) \circ x^{-1}\) follows by a similar argument. \(\square\)

**Theorem 3.3.5.** Let \(Q\) be a semiautomorphic IP loop, \(g_0 \in Z(Q)\), and \(\ast\) an involutory antiautomorphism of \(G\) such that \(g^* = g_0g^g \in Z(Q)\) for every \(g \in Q\). For an indeterminate \(t\), define multiplication \(\circ\) on \(Q \cup Qt\) by

\[
g \circ h = gh, \quad g \circ (ht) = (hg)t, \quad gt \circ h = (gh^*)t, \quad gt \circ ht = g_0h^*g,
\]

where \(g, h \in Q\). Then \((Q \cup Qt, \circ)\) is a semiautomorphic IP loop.
Proof. We see that by letting \( * \) be an involutory antiautomorphism, (3.3.4.1), (3.3.4.2) and (3.3.4.3) of Lemma 3.3.4 are satisfied. Note that multiplication in Lemma 3.3.4 becomes the multiplication in Theorem 3.3.5.

\[ \]

### 3.3.2 Generalizing de Barros-Juriaans’ Construction

We now give our second construction, which is based on another doubling technique of de Barros and Juriaans. It was already noted (without human proof) that applying the de Barros-Juriaans construction to a group gives what we are now calling a semiautomorphic IP loop. Here we show that just as with the Chein construction, starting with a semiautomorphic IP loop in the de Barros-Juriaans construction yields another semiautomorphic IP loop (Theorem 3.3.6).

**Theorem 3.3.6.** Let \( Q \) be a semiautomorphic IP loop, \( g_0 \in Z(Q) \), and \( * \) an involutory antiautomorphism of \( Q \) such that \( g_0^* = g_0, gg^* \in Z(Q) \) for every \( g \in Q \). For an indeterminate \( t \), define multiplication \( \circ \) on \( Q \cup Qt \) by

\[
g \circ h = gh, \quad g \circ (ht) = (gh)t, \quad gt \circ h = (h^*g)t, \quad gt \circ ht = g_0gh^*,
\]

where \( g, h \in Q \). Then \( (Q \cup Qt, \circ) \) is a semiautomorphic IP loop.

**Proof.** As before, we consider eight cases.

**Case 1.** \( x, y, z \in Q \). Then we are finished.

**Case 2.** \( x, y \in Q \) and \( z \in Qt \), so let \( x = g, y = h, z = kt \) for some \( g, h, k \in Q \). Thus

\[
(x \circ y) \circ (z \circ (x \circ y)) = (g \circ h) \circ (kt \circ (g \circ h)) = gh \circ ((gh)^* \cdot k)t
\]

61
\( (gh \cdot ((gh)^* \cdot k))t \)

\[ = (gh \cdot ((gh)^* \cdot k))t \]

(3.3.2.2)

\[ = ((gh \cdot (gh)^*)k)t \]

(3.3.2.3)

\[ = (gh \cdot h^* g^*)tk \]

\[ = ((gh \cdot h^* g^*)g^*)tk \]

\[ = ((gh \cdot h^* g^*)k)t \]

\[ = (g^* g \cdot (h^* h \cdot k))t \]

\[ = (h^* (g^* g \cdot h k))t \]

(3.3.2.2)

\[ = (h^* (g^* (g \cdot h k)))t \]

\[ = (g^* (g \cdot h k))t \circ h \]

\[ = (((g \cdot h k)t) \circ g) \circ h \]

\[ = ((g \circ (h k)t) \circ g) \circ h \]

\[ = ((g \circ (h \circ k t)) \circ g) \circ h \]

\[ = ((x \circ (y \circ z)) \circ x) \circ y. \]

**Case 3.** \( x, z \in Q \) and \( y \in Q_t \), so let \( x = g, y = ht, z = k \) for some \( g, h, k \in Q \). Thus

\( (x \circ y) \circ (z \circ (x \circ y)) = (g \circ ht) \circ (k \circ (g \circ ht)) \)

\[ = (gh)t \circ (k \circ (gh)t) \]

\[ = (gh)t \circ (k \cdot gh)t \]

\[ = g_0(gh \cdot (k \cdot gh)^*) \]

\[ = g_0(gh \cdot ((gh)^* \cdot k^*)) \]

\[ = g_0((gh \cdot (gh)^*)k^*) \]
\[= g_0(gh \cdot h^*g^*)k\]
\[= g_0((gh^*) \cdot g^*)k\]
\[= g_0(hh^*gg^*)k\]
\[= g_0(gg^*(k \cdot hh^*))\]
\[= g_0((k \cdot gg^*)h^*)\]
\[= g_0((g^*g \cdot k^*h)h^*)\]
\[= g_0((g^*g \cdot k^*h)h^*)\]
\[= (g^*(g \cdot k^*h))h^*\]
\[= ((g^*(g \cdot k^*h))h^*)\]
\[= ((g^*(g \cdot k^*h))h^*)\]
\[= ((x \circ y \circ z) \circ x) \circ y.\]

**Case 4.** \( y, z \in Q \) and \( x \in Q_t \), so let \( x = gt, y = h, z = k \) for some \( g, h, k \in Q \). Thus

\[(x \circ y) \circ (z \circ (x \circ y)) = (gt \circ h) \circ (k \circ (gt \circ h))\]
\[= (h^*g)t \circ (k \circ (h^*g)t)\]
\[= (h^*g)t \circ (k \cdot h^*g)t\]
\[= g_0(h^*g) \cdot (k 
\cdot h^*g)^*\]
\[= g_0((h^*g) \cdot ((h^*g)^* \cdot k^*))\]
\[= g_0((h^*g)^* \cdot (k^*h^*g)^*)\]
\[= g_0((h^*g \cdot g^*h)^*k^*)\]
\[(3.3.2.3)\]
\[= g_0((h^* \cdot gg^*)h \cdot k^*)\]
\[= g_0((gg^* \cdot hh^*)k^*)\]
\[= g_0((k^* \cdot h^*)h \cdot gg^*)\]
\[(3.3.2.2)\]
\[= g_0((k^* h^* \cdot h) \cdot gg^*)\]
\[= g_0(k^* h^* \cdot gg^*)h\]
\[(3.3.2.1)\]
\[= g_0((k^* h^* \cdot g)g^*)h\]
\[= g_0(((hk)^* \cdot g)g^*)h\]
\[= (((hk)^* g) t \circ gt)h\]
\[= ((gt \circ hk) \circ gt) \circ h\]
\[= ((x \circ (y \circ z)) \circ x) \circ y.\]

**Case 5.** \(z \in Q\) and \(x, y \in Qt\), so let \(x = gt, y = ht, z = k\) for some \(g, h, k \in Q\). Thus

\[(x \circ y) \circ (z \circ (x \circ y)) = (gt \circ ht) \circ (k \circ (gt \circ ht))\]
\[= g_0(gh^*) \circ (k \circ g_0(gh^*))\]
\[= g_0g_0(gh^* \cdot (k \cdot gh^*))\]
\[= g_0g_0((g \cdot (k^* h^*)g) \cdot h^*)\]
\[= g_0(((g \cdot (k^* h^*)g) t \circ ht)\]
\[= g_0((g \cdot (k^* h^*)) \circ gt) \circ ht\]
\[= ((gt \circ (k^* h)) \circ gt) \circ ht\]
\[= (gt \circ ((ht \circ k) \circ gt)) \circ ht\]

64
\((x \circ (y \circ z)) \circ x \circ y.\)

**Case 6.** \(x, z \in Q\) and \(y \in Q_t\), so let \(x = gt, y = h, z = kt\) for some \(g, h, k \in Q\). Thus

\[
(x \circ y) \circ (z \circ (x \circ y)) = (gt \circ h) \circ (kt \circ (gt \circ h))
\]

\[
= (\(h^* \cdot (h^*)^* \cdot (h^* \cdot (h^* g)) \cdot \) t)
\]

\[
= g_0((h^* g) \circ k \cdot (h^* g)^*)
\]

\[
= g_0((k \cdot (h^* g)^*)^* \cdot h^* g) \cdot t
\]

\[
= g_0(h^* \cdot g \cdot \cdot k \cdot (h^* g)^* \cdot h^* g) \cdot t
\]

\[
= g_0(h^* \cdot g \cdot (hk)^*) \cdot h^* g) \cdot t
\]

\[
= g_0(g \cdot (hk)^*) \circ h \cdot t
\]

\[
= g_0((g \cdot (hk)^*) \circ g t) \circ h
\]

\[
= ((gt \circ (hk) t) \circ g t) \circ h
\]

\[
= ((gt \circ (h \circ kt)) \circ g t) \circ h
\]

\[
= ((x \circ (y \circ z)) \circ x) \circ y.
\]

**Case 7.** \(x \in Q\) and \(y, z \in Q_t\), so let \(x = g, y = ht, z = kt\) for some \(g, h, k \in Q\). Thus

\[
(x \circ y) \circ (z \circ (x \circ y)) = (g \circ h t) \circ (kt \circ (g \circ h t))
\]

\[
= (gh) \circ (kt \circ (gh) t)
\]

\[
= g_0((gh) t \circ (k \cdot (gh)^*))
\]

\[
= g_0((k \cdot (gh)^*)^* \cdot (gh) t)
\]

\[
= g_0((gh \cdot k^*) \cdot gh) t
\]

65
\[(\text{RIF}1)\quad = g_0((g \cdot (hk^*)g \cdot h)t)\]
\[= g_0(((g \circ hk^*) \circ g) \circ ht)\]
\[= ((g \circ (ht \circ kt)) \circ g) \circ ht\]
\[= ((x \circ (y \circ z)) \circ x) \circ y.\]

**Case 8.** $x, y, z \in Qt$, so let $x = gt, y = ht, z = kt$ for some $g, h, k \in Q$. Thus

\[(x \circ y) \circ (z \circ (x \circ y)) = (gt \circ ht) \circ (kt \circ (gt \circ ht))\]
\[= g_0g_0((gh^* \circ (kt \circ gh^*))t)\]
\[= g_0g_0((gh^* \circ ((gh^*)^*k)t)\]
\[= g_0g_0((gh^* \cdot (gh^*)^*k)t\]
\[= g_0g_0((gh^* \cdot h^g^*)k)t\]
\[= g_0((g^*g \cdot h^*h)k)t\]
\[= g_0((k \cdot h^*h) \cdot g^*g^*)t\]
\[= g_0((kh^* \cdot g^*g^*)h)t\]
\[= g_0g_0((kh^* \cdot g)g^* \cdot h)t\]
\[= g_0(((hk^*)^* \cdot g)t \circ gt) \circ ht\]
\[= g_0((gt \circ (hk^*)) \circ gt) \circ ht\]
\[= ((gt \circ (ht \circ kt)) \circ gt) \circ ht\]
\[= ((x \circ (y \circ z)) \circ x) \circ y.\]
The argument for IP is similar to the argument in Theorem 3.3.5.

3.4 Connections between the extended Chein and extended de Barros-Juriaans constructions

Proposition 3.4.1. Let $Q$ be a semiautomorphic IP loop and let $g_0 \in Z(Q)$. Then $g_0 \in Z(Q \cup Qt, \circ)$ in either construction.

Proof. Suppose $(Q \cup Qt, \circ)$ has the multiplication as in Theorem (3.3.5) and let $g_0 \in Z(Q)$. First note

$$g_0 \circ ht = (hg_0)t = (h g_0^*)t = ht \circ g_0.$$

Hence, $g_0 \in C(Q \cup Qt)$. Now, let $x, y \in Q \cup Qt$. It is enough to show $g_0 \circ (x \circ y) = (g_0 \circ x) \circ y$ and $x \circ (y \circ g_0) = (x \circ y) \circ g_0$. We have the following cases:

Case 1. $x, y \in Q$, so we are done.

Case 2. $x \in Q$ and $y \in Qt$, so let $x = g, y = ht$ for some $g, h \in Q$. Thus

$$g_0 \circ (g \circ ht) = g_0 \circ (hg)t = (hg \cdot g_0)t = (h \cdot g_0^*)t = g_0 g \circ ht = (g_0 \circ g) \circ ht,$$

$$g \circ (ht \circ g_0) = g \circ (hg_0)t = (hg_0 \cdot g)t = (hg \cdot g_0)t = (hg)t \circ g_0 = (g \circ ht) \circ g_0.$$

Case 3. $x \in Qt$ and $y \in Q$, so let $x = gt, y = h$ for some $g, h \in Q$. Thus

$$g_0 \circ (gt \circ h) = g_0 \circ (gh^*)t = (g_0 \cdot gh^*)t = (gg_0 \cdot h^*)t = (gg_0) \circ h = (g_0 \circ gt) \circ h,$$

$$gt \circ (h \circ g_0) = gt \circ (h g_0) = (g \cdot h^* g_0)t = (gh^* \cdot g_0)t = (gh^*)t \circ g_0 = (gt \circ h) \circ g_0.$$
Case 4. $x \in Qt$ and $y \in Qt$, so let $x = gt, y = ht$ for some $g, h \in Q$. Thus

$$g_0 \circ (gt \circ ht) = g_0 \circ g_0(h^*g) = g_0 \cdot g_0(h^*g) = (gg_0)t \circ ht = (g_0 \circ gt) \circ ht,$$

$$gt \circ (ht \circ g_0) = gt \circ (hg_0)t = g_0 \cdot (hg_0)^*g = g_0 \cdot (h^*g_0 \cdot g) = (g_0 \cdot h^*g_0)g = (gt \circ ht) \circ g_0.$$

The argument is similar if the multiplication is defined as in Theorem (3.3.6).

Proposition 3.4.2. Let $Q$ be a semiautomorphic IP loop and $*$ an antiautomorphism of $Q$. Reusing the symbol $*$, we extend $*$ on $Q \cup Qt$ as

$$g^* = g^*,$$

$$(gt)^* = gt.$$

Then in either construction, the extend $*$ is an antiautomorphism of $(Q \cup Qt, \circ)$.

Proof. Suppose $(Q \cup Qt, \circ)$ has the multiplication as in Theorem (3.3.5) and let $x, y \in Q \cup Qt$. Then we have the 4 following cases:

Case 1. $x, y \in Q$, so we are done.

Case 2. $x \in Q$ and $y \in Qt$, so let $x = g, y = ht$ for some $g, h \in Q$. Thus

$$(g \circ ht)^* = ((hg)t)^* = (hg)t = ht \circ g^* = (ht)^* \circ g^*.$$

Case 3. $x \in Qt$ and $y \in Q$, so let $x = gt, y = h$ for some $g, h \in Q$. Thus

$$(gt \circ h)^* = ((gh^*)t)^* = (gh^*)t = h^* \circ gt = h^* \circ (gt)^*.$$
Case 4. \( x \in Qt \) and \( y \in Qt \), so let \( x = gt, y = ht \) for some \( g, h \in Q \). Thus

\[
(gt \circ ht)^* = (g_0 h^* g)^* = g_0 g^* h = ht \circ gt = (ht)^* \circ (gt)^*.
\]

The argument is similar if the multiplication is define as in Theorem (3.3.6).

Theorem 3.4.3. Let \( Q \) be a semiautomorphic IP loop with \( g_0 = 1 \) and \( * \) an anti-automorphism (which we can extend by Proposition (3.4.2)). Let \( Q_1 = (Q \cup Qs, \circ) \) with multiplication from Theorem 3.3.6 and \( Q_2 = (Q \cup (Qs)t) \) where we apply the multiplication from Theorem 3.3.5 twice. Then \( Q_1 \cong Q_2 \).

Proof. Note the multiplication in \( Q_2 \) is as follows (where we reuse \( \circ \) for both multiplications):

\[
g \circ_2 h = gh
\]

\[
g \circ_2 (hs)t = (hs \circ g)t = ((hg^*)s)t,
\]

\[
(gs)t \circ_2 h = (gs \circ h^*)t = ((gh)s)t,
\]

\[
(gs)t \circ_2 (hs)t = ((hs)^* \circ gs) = (g^*h).
\]

<table>
<thead>
<tr>
<th>( Q_2, \circ_2 )</th>
<th>( h )</th>
<th>( (hs)t )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( g )</td>
<td>( gh )</td>
<td>( ((hg^*)s)t )</td>
</tr>
<tr>
<td>( (gs)t )</td>
<td>( ((gh)s)t )</td>
<td>( (g^*h) )</td>
</tr>
</tbody>
</table>

Table 3.1: Multiplication Table for \( (Q_2, \circ_2) \)

Consider the bijection \( \phi : Q_1 \mapsto Q_2 \) by

\[
g\phi = g \quad (gs)\phi = (g^*s)t.
\]
To show \((x \circ_1 y)\phi = x\phi \circ_2 y\phi\), we have 4 cases.

Case 1. \(x, y \in Q\), so let \(x = g, y = h\) for some \(g, h \in Q\). Thus

\[
(g \circ_1 h)\phi = (gh)\phi = gh = g\phi \circ_2 h\phi.
\]

Case 2. \(x \in Q\) and \(y \in Qt\), so let \(x = g, y = hs\) for some \(g, h \in Q\). Thus

\[
(g \circ_1 hs)\phi = ((gh)s)\phi = ((gh)^* s)t = ((h^* g^*)s)t = g \circ_2 (h^* s)t = g\phi \circ_2 (hs)\phi.
\]

Case 3. \(x \in Qs\) and \(y \in Q\), so let \(x = gs, y = h\) for some \(g, h \in Q\). Thus

\[
(gs \circ_1 h)\phi = ((h^* g)s)\phi = ((h^* g)^* s)t = ((g^* h)s)t = (g^* s)t \circ_2 h = (gs)\phi \circ_2 h\phi.
\]

Case 4. \(x \in Qs\) and \(y \in Qs\), so let \(x = gs, y = hs\) for some \(g, h \in Q\). Thus

\[
(gs \circ_1 hs)\phi = (gh^*)\phi = (g^* s)t \circ_2 (h^* s)t = (gs)\phi \circ_2 (hs)\phi.
\]

\(\square\)

**Proposition 3.4.4.** Let \(Q\) be a semiautomorphic IP loop and \(\ast\) an antiautomorphism of \(Q\). Let \(c \in Z(Q)\) such that \(c^2 = 1\) and \(c^\ast = c\). Then, reusing the symbol \(\ast\), we extend \(\ast\) on \(Q \cup Qt\) as

\[
g^\ast = g^\ast,
\]

\[
(gt)^\ast = c \cdot gt.
\]
Then in either construction, the extend $*$ is an antiautomorphism of $(Q \cup Qt, \circ)$.

**Proof.** Suppose $(Q \cup Qt, \circ)$ has the multiplication as in Theorem (3.3.5) and let $x, y \in Q \cup Qt$. Then we have the 4 following cases:

**Case 1.** $x, y \in Q$, so we are done.

**Case 2.** $x \in Q$ and $y \in Qt$, so let $x = g, y = ht$ for some $g, h \in Q$. Thus

$$(g \circ ht)^* = ((hg)t)^* = c \cdot (hg)t = ht \circ g^* = (ht)^* \circ g^*.$$ 

**Case 3.** $x \in Qt$ and $y \in Q$, so let $x = gt, y = h$ for some $g, h \in Q$. Thus

$$(gt \circ h)^* = ((gh^*)t)^* = c \cdot (gh^*)t = h^* \circ (c \cdot gt) = h^* \circ (gt)^*.$$ 

**Case 4.** $x \in Qt$ and $y \in Qt$, so let $x = gt, y = ht$ for some $g, h \in Q$. Thus

$$(gt \circ ht)^* = (g0h^*)^* = g0g^*h = (c \cdot ht) \circ (c \cdot gt) = (ht)^* \circ (gt)^*.$$ 

The argument is similar if the multiplication is define as in Theorem (3.3.6). $\Box$

**Theorem 3.4.5.** Let $Q$ be a semiautomorphic IP loop with $g_0 \in Q$, $g_0^2 = 1$ and $*$ an antiautomorphism extending as in Proposition 3.4.4. Then doubling $Q$ twice first using the multiplication in Theorem 3.3.6 followed by the multiplication in Theorem 3.3.5 is equivalent to doubling $Q$ twice using the multiplication in Theorem 3.3.5 twice.

**Proof.** Let

$$Q_1 = ((Q \cup Qs) \cup (Q \cup Qs)t, \circ_1) = (Q \cup Qs \cup Qt \cup (Qs)t, \circ_1)$$
be the loop formed by first using the doubling construction in Theorem 3.3.6 and then doubled again using the multiplication in Theorem 3.3.5. Similarly, define

\[ Q_2 = ((Q \cup Qs) \cup (Q \cup Qs)t, \circ_2) = (Q \cup Qs \cup Qt \cup (Qs)t, \circ_2) \]

where we double \( Q \) twice using the multiplication in Theorem 3.3.5 twice. Then we have the following tables.

### Table 3.2: Multiplication Table for \((Q_1, \circ_1)\).

<table>
<thead>
<tr>
<th>((Q_1, \circ_1))</th>
<th>(h)</th>
<th>(hs)</th>
<th>(ht)</th>
<th>((hs)t)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(g)</td>
<td>(gh)</td>
<td>((gh)s)</td>
<td>((hg)t)</td>
<td>(((g^*hs)t))</td>
</tr>
<tr>
<td>(gs)</td>
<td>((gh^*)s)</td>
<td>(g_0((gh^*)t))</td>
<td>(((gh)s)t)</td>
<td>(((g^*hs)g_0))</td>
</tr>
<tr>
<td>(gt)</td>
<td>((gh^*)t)</td>
<td>([g_0((gh)s)t)</td>
<td>(g_0(h^*g))</td>
<td>(((g^*hs)t))</td>
</tr>
<tr>
<td>((gs)t)</td>
<td>(((gh)s)t)</td>
<td>(gh^*t)</td>
<td>(g_0((g^*hs))</td>
<td>(g_0(h^*gs))</td>
</tr>
</tbody>
</table>

### Table 3.3: Multiplication Table for \((Q_2, \circ_2)\).

<table>
<thead>
<tr>
<th>((Q_2, \circ_2))</th>
<th>(h)</th>
<th>(hs)</th>
<th>(ht)</th>
<th>((hs)t)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(g)</td>
<td>(gh)</td>
<td>((gh)s)</td>
<td>((hg)t)</td>
<td>(((hg)s)t)</td>
</tr>
<tr>
<td>(gs)</td>
<td>((gh^*)s)</td>
<td>(g_0(h^*g))</td>
<td>(((gh)s)t)</td>
<td>((g_0 \cdot g^*ht))</td>
</tr>
<tr>
<td>(gt)</td>
<td>((gh^*)t)</td>
<td>([g_0((gh)s)t]</td>
<td>(g_0(h^*g))</td>
<td>(((g^*hs)t))</td>
</tr>
<tr>
<td>((gs)t)</td>
<td>(((gh)s)t)</td>
<td>(h^*g)</td>
<td>(g_0((g^*hs))</td>
<td>(g_0(g^*h))</td>
</tr>
</tbody>
</table>

Consider the bijection \(\phi : Q_1 \rightarrow Q_2\) defined as:

\[ g \phi = g \quad (gs) \phi = (g^*s)t \quad (gt) \phi = g_0 \cdot gt \quad ((gs)t) \phi = g^*s. \]

To see that \(\phi\) is indeed an isomorphism, we have the following 16 cases:

**Case 1.** \(x, y \in Q\), so let \(x = g, y = h\) for some \(g, h \in Q\). Thus

\[ (g \circ_1 h) \phi = (gh) \phi = gh = g \phi \circ_2 h \phi. \]
Case 2. $x \in Q$ and $y \in Qs$, so let $x = g, y = hs$ for some $g, h \in Q$. Thus

$$(g \circ_1 hs) \phi = ((gh)s) \phi = ((gh)^s)t = ((h^*g^*)s)t = g \circ_2 (h^*s)t = g \phi \circ_2 (hs) \phi.$$ 

Case 3. $x \in Qs$ and $y \in Q$, so let $x = gs, y = h$ for some $g, h \in Q$. Thus

$$(gs \circ_1 h) \phi = ((h^*g)s) \phi = ((h^*g)^s)t = ((g^*h)s)t = (g^*s)t \circ_2 h = (gs) \phi \circ_2 h \phi.$$ 

Case 4. $x \in Qs$ and $y \in Qs$, so let $x = gs, y = hs$ for some $g, h \in Q$. Thus

$$(gs \circ_1 hs) \phi = (g_0 \cdot gh^*) \phi = g_0 \cdot gh^* = g^3_0 \cdot gh^* = (g_0 \cdot g^*s)t \circ_2 (g_0 \cdot h^*s)t$$

$$= (gs) \phi \circ_2 (hs) \phi.$$ 

Case 5. $x \in Qt$ and $y \in Q$, so let $x = gt, y = h$ for some $g, h \in Q$. Thus

$$(gt \circ_1 h) \phi = ((gh^*)t) \phi = g_0 \cdot (gh^*)t = g_0 (gt) \circ_2 h = (gt) \phi \circ_2 h \phi.$$ 

Case 6. $x \in Q$ and $y \in Qt$, so let $x = g, y = ht$ for some $g, h \in Q$. Thus

$$(g \circ_1 ht) \phi = ((hg)t) \phi = g_0 \cdot (hg)t = g \circ_2 (g_0 \cdot ht) = g \phi \circ_2 (ht) \phi.$$ 

Case 7. $x \in Qt$ and $y \in Qt$, so let $x = gt, y = ht$ for some $g, h \in Q$. Thus

$$(gt \circ_1 ht) \phi = (g_0 \cdot h^*g) \phi = g_0 h^*g = g_0 (gt) \circ_2 g_0 (ht) = (gt) \phi \circ_2 (ht) \phi.$$
Case 8. $x \in Q_s$ and $y \in Q_t$, so let $x = gs, y = ht$ for some $g, h \in Q$. Thus

$$(gs \circ_1 ht)\phi = [(hg)s]t\phi = (hg)^* = g_0^2 \cdot (g^*h^*)s = (g^*s)t \circ_2 (g_0 \cdot ht) = (gs)\phi \circ_2 (ht)\phi.$$  

Case 9. $x \in Q_s$ and $y \in (Qs)t$, so let $x = gs, y = (hs)t$ for some $g, h \in Q$. Thus

$$(gs \circ_1 (hs)t)\phi = ((g_0 \cdot hg^*)t)\phi = g_0^2 \cdot (hg^*)t = (g^*s)t \circ_2 (h^*s) = (gs)\phi \circ_2 ((hs)t)\phi.$$  

Case 10. $x \in Q_t$ and $y \in Q_s$, so let $x = gt, y = ht$ for some $g, h \in Q$. Thus

$$(gt \circ_1 hs)\phi = (((g_0 \cdot gh)\phi)s)\phi = g_0\cdot (gh)^*s = g_0^2 \cdot (h^*g^*)s = (g_0 \cdot gt) \circ_2 (h^*s)t = (gt)\phi \circ_2 (hs)\phi.$$  

Case 11. $x \in Q_t$ and $y \in (Qs)t$, so let $x = gt, y = (hs)t$ for some $g, h \in Q$. Thus

$$(gt \circ_1 (hs)t)\phi = (g_0^2 \cdot (g^*h)s)\phi = ((h^*g)s)t = (g_0 \cdot gt) \circ_2 (h^*s) = (gt)\phi \circ_2 ((hs)t)\phi.$$  

Case 12. $x \in (Qs)t$ and $y \in Q_s$, so let $x = (gs)t, y = hs$ for some $g, h \in Q$. Thus

$$((gs)t \circ_1 hs)\phi = (gh^*)t\phi = g_0 \cdot (gh^*)t = g_0 \cdot (gh^*)t = (g^*s) \circ_2 (h^*s)t = ((gs)t)\phi \circ_2 (hs)\phi.$$  

Case 13. $x \in (Qs)t$ and $y \in Q_t$, so let $x = (gs)t, y = ht$ for some $g, h \in Q$. Thus

$$((gs)t \circ_1 ht)\phi = (g_0 \cdot (h^*g)s)\phi = g_0 \cdot ((h^*g)^*s)t = g_0 \cdot ((h^*g)s)t = (g^*s) \circ_2 (g_0 \cdot ht) = ((gs)t)\phi \circ_2 (ht)\phi.$$  

74
Case 14. \( x \in (Qs)t \) and \( y \in (Qs)t \), so let \( x = (gs)t, y = (hs)t \) for some \( g, h \in Q \). Thus

\[
((gs)t \circ_1 (hs)t) \phi = (g_0 \cdot h^*) \phi = g_0 \cdot h^* = (g^*s) \circ_2 (h^*s) = ((gs)t) \phi \circ_2 ((hs)t) \phi.
\]

Case 15. \( x \in (Qs)t \) and \( y \in Q \), so let \( x = (gs)t, y = h \) for some \( g, h \in Q \). Thus

\[
((gs)t \circ_1 h) \phi = (((hs)s)t) \phi = (h^*s) = (g^*h^*)s = (g^*s) \circ_2 h = ((gs)t) \phi \circ_2 h \phi.
\]

Case 16. \( x \in Q \) and \( y \in (Qs)t \), so let \( x = g, y = (hs)t \) for some \( g, h \in Q \). Thus

\[
(g \circ_1 (hs)t) \phi = (((g^*h)s)t) \phi = (g^*h^*)s = (h^*g)s = g \circ_2 (h^*s) = g \phi \circ_2 ((hs)t) \phi.
\]

\[\Box\]

3.5 Conclusion

A loop \( Q \) is a C-loop if \( C_0(Q) = Q \) (i.e. \( x \cdot y(yz) = (xy)y \cdot z \) holds for all \( x, y, z \)). Since C-loops are closely related to Moufang and Steiner loops, it is natural to see examples of C-loops arise in this context.

Theorem 3.5.1. Let \( Q \) be a semiautomorphic IP loop, \( g_0 \in Z(Q) \), and \( * \) an involutory antiautomorphism of \( Q \) such that \( g_0^* = g_0, gg^* \in Z(Q) \) for every \( g \in Q \). Then, using either multiplication in Theorem 3.3.5 or 3.3.6, the following are equivalent:

(i) \( (Q \cup Qt, \circ) \) is commutative.

(ii) \( g^* = g \) for all \( g \in Q \).
Moreover, if either hold, then \( g^2 \in Z(Q) \) for all \( g \in Q \) and \( Q \) is a commutative C-loop.

**Proof.** Let \((Q \cup Q_t, \circ)\) have the multiplication from Theorem 3.3.5. If \((Q \cup Q_t, \circ)\) is commutative, then \((gh^*)t = gt \circ h = h \circ gt = (gh)t\). Letting \( g = 1 \), we have the desired result. Alternatively, \( * \) is antiautomorphism of \( Q \), and since \( g^* = g \), we have \( hg = h^*g^* = (gh)^* = gh \). Hence, \((Q \cup Q_t, \circ)\) is commutative. Finally, if either (i) or (ii) holds, then \( g^2 = gg^* \in Z(Q) \) for all \( g \in Q \). Therefore, by [11] and the fact that \( Q \) is an IP loop, \( Q \) is a commutative C-loop.

**Example 3.5.2.** Let \( Q \) be the Steiner loop of order 16 with GAP library number [16;2]. Then \(|Z(Q)| = 2\). Let \( g_0 \in Z(Q) \), \( g_0 \neq 1 \) and \( g^* = g^{-1} \). Then \((Q \cup Q_t, \circ)\) is a commutative C-loop.

**Corollary 3.5.3.** Let \( Q \) be a Steiner loop. Then, for either multiplication in Theorem 3.3.5 or 3.3.6, if \((Q \cup Q_t, \circ)\) is a Steiner loop, then \((Q \cup Q_t, \circ) \cong Q \times Q\).

**Proof.** Let \((Q \cup Q_t, \circ)\) have the multiplication from Theorem 3.3.5. If \((Q \cup Q_t, \circ)\) is Steiner, hence commutative, then \( g^* = g \) by Theorem 3.5.1. Moreover, \( 1 = gt \circ gt = g_0(g^*g) = g_0(g^2) = g_0 \).

Recall that semiautomorphic IP loops are generalized by flexible loops satisfying (ARIF). Hence, it is natural to ask what \((Q \cup Q_t, \circ)\) would be if \( Q \) started as a flexible loop satisfying (ARIF).

**Theorem 3.5.4.** Let \( Q \) be a flexible loop satisfying (ARIF), \( g_0 \in Z(Q) \), and \( * \) an involutory antiautomorphism of \( Q \) such that \( g_0^* = g_0, gg^* \in Z(Q) \) for every \( g \in Q \). For an indeterminate \( t \), define multiplication \( \circ \) on \( Q \cup Q_t \) by either multiplication in Theorem 3.3.5 or 3.3.6. Then \((Q \cup Q_t, \circ)\) is a flexible loop satisfying (ARIF).
Proof. **Case 1a** \(x, y, z \in G\). Then we are finished.

**Case 2a** \(x, y \in G\) and \(z \in Gt\), so let \(x = g, y = h, z = kt\). Thus

\[
(z \circ x) \circ (y \circ x \circ y) = (kt \circ g) \circ (hgh)
\]
\[
= (kg^*)t \circ (h \circ g \circ h)
\]
\[
= (kg^* \circ (hgh^*))t
\]
\[
= (kg^* \cdot (h^*g^*h^*))t
\]
\[
\overset{(ARIF)}{=} (k(g^*h^*g^*) \cdot h^*)t
\]
\[
= (k(ghg)^* \cdot h^*)t
\]
\[
= (k(ghg)^*)t \circ h
\]
\[
= (kt \circ (ghg)) \circ h
\]
\[
= (z \circ (x \circ y \circ x)) \circ y.
\]

**Case 3a** \(x, z \in G\) and \(y \in Gt\), so let \(x = g, y = ht, z = k\). Thus

\[
(z \circ x) \circ (y \circ x \circ y) = (k \circ g) \circ (ht \circ g \circ ht)
\]
\[
= kg \circ (ht \circ (hg)t)
\]
\[
= g_0(kg \circ (hg)^*h)
\]
\[
= g_0(kg \cdot (g^*h^* \cdot h))
\]
\[
\overset{(3.3.2.1)}{=} g_0(kg \cdot (g^* \cdot h^*h))
\]
\[
= g_0((kg \cdot g^*) \cdot h^*h)
\]
\[
\overset{(3.3.2.1)}{=} g_0((k \cdot g^*) \cdot h^*h)
\]
\[
= g_0(gg^* \cdot (h^*h \cdot k))
\]
\[ \begin{align*}
(3.3.2.2) \quad & = g_0(gg^* \cdot (h^* \cdot hk)) \\
& = g_0(h^* \cdot (h \cdot gg^*)k) \\
(3.3.2.1) \quad & = g_0(h^* \cdot (hg^* g)k) \\
& = ((hg \cdot g^*)k) \circ ht \\
& = (k \circ (hg \cdot g^*)t) \circ ht \\
& = (k \circ ((hg)t \circ h)) \circ ht \\
& = (k \circ (g \circ ht \circ g)) \circ ht \\
& = ((z \circ (x \circ y \circ x)) \circ y).
\end{align*} \]

**Case 4a** \( y, z \in G \) and \( x \in G_t \), so let \( x = gt, y = h, z = k \). Thus

\[ (z \circ x) \circ (y \circ x \circ y) = (k \circ gt) \circ (h \circ gt \circ h) \]
\[ = (gk)t \circ (h \circ gt \circ h) \]
\[ = (gk)t \circ ((gh)t \circ h) \]
\[ = (gk)t \circ (gh \cdot h^*)t \]
\[ = g_0((gh \cdot h^*)^* \cdot gk) \]
\[ = g_0((h \cdot h^* g^*) \cdot gk) \]
\[ (3.3.2.2) \quad = g_0((hh^* \cdot g^*) \cdot gk) \]
\[ = g_0(hh^* \cdot (g^* \cdot gk)) \]
\[ (3.3.2.2) \quad = g_0(hh^* \cdot (g^* \cdot g \cdot k)) \]
\[ = g_0((k \cdot h^* h) \cdot g^* g) \]
\[ (3.3.2.2) \quad = g_0((kh^* \cdot h) \cdot g^* g) \]
\[= g_0((k(h^*g)\cdot h))\]

\[(3.3.2.1)\]

\[= g_0((k(h^*g)\cdot h))\]

\[= g_0((k((gh)^*g)\cdot h))\]

\[= (k \circ (gt \circ (gh)t)) \circ h\]

\[= (k \circ (gt \circ h \circ gt)) \circ h\]

\[= (z \circ (x \circ y \circ x)) \circ y.\]

**Case 5a** \(z \in G\) and \(x, y \in Gt\), so let \(x = gt, y = ht, z = k\). Thus

\[= g_0((k(h \circ g \cdot g) \cdot h))\]

\[(ARIF)\]

\[= g_0((k(h \circ g \cdot g) \cdot h))\]

\[= g_0((k((gh)^*g)\cdot h))\]

\[= (k \circ (gt \circ (gh)t)) \circ h\]

\[= (k \circ (gt \circ h \circ gt)) \circ h\]

\[= (z \circ (x \circ y \circ x)) \circ y.\]
Case 6a $x, z \in G$ and $y \in Gt$, so let $x = gt, y = h, z = kt$. Thus

$$(z \circ x) \circ (y \circ x \circ y) = (kt \circ gt) \circ (h \circ gt \circ h)$$

$$= g_0(g^*k \circ (h \circ gt \circ h))$$

$$= g_0(g^*k \circ (h \circ (gh^*)t))$$

$$= g_0(g^*k \circ (gh^* \cdot h)t)$$

$$= g_0((gh^* \cdot h) \cdot g^*k)t$$

$$\overset{(3.3.2.1)}{=} g_0((g \cdot h^*h) \cdot g^*k)t$$

$$= g_0(h^*h \cdot (g \cdot g^*k))t$$

$$\overset{(3.3.2.2)}{=} g_0(h^*h \cdot (gg^* \cdot k))t$$

$$= g_0((kh \cdot h^*) \cdot gg^*)t$$

$$\overset{(3.3.2.1)}{=} g_0((kh \cdot h^*) \cdot gg^*)t$$

$$= g_0(k(gg^* \cdot h) \cdot h^*)t$$

$$\overset{(3.3.2.2)}{=} g_0(k(g \cdot g^*h) \cdot h^*)t$$

$$= g_0(k(h^*g^* \cdot g) \cdot h^*)t$$

$$= g_0(k((gh)^* \cdot g)^* \cdot h^*)t$$

$$= g_0((k((gh)^* \cdot g)t \circ h)$$

$$= g_0((kt \circ ((gh)^* \cdot g)) \circ h)$$

$$= (kt \circ (gt \circ (gh)t)) \circ h$$

$$= (kt \circ (gt \circ h \circ gt)) \circ h$$

$$= (z \circ (x \circ y \circ x)) \circ y.$$
Case 7a $x \in G$ and $y, z \in Gt$, so let $x = g, y = ht, z = kt$. Thus

$$(z \circ x) \circ (y \circ x \circ y) = (kt \circ g) \circ (ht \circ g \circ ht)$$

$$= (kg^*) \circ (ht \circ g \circ ht)$$

$$= (kg^*) \circ ((hg^*) \circ ht)$$

$$= g_0((kg^*) \circ (h^* \cdot hg^*))$$

$$= g_0(kg^* \cdot (h^* \cdot hg^*))t$$

$$= g_0(kg^* \cdot (gh^* \cdot h))t$$

$$(3.3.2.1) \quad \Rightarrow \quad g_0(kg^* \cdot (g \cdot h^* h))t$$

$$= g_0((kg^* \cdot g) \cdot h^* h)$$

$$(3.3.2.1) \quad \Rightarrow \quad g_0((k \cdot g^* g) \cdot h^* h)$$

$$= g_0(g^* g \cdot (h h^* k))$$

$$(3.3.2.2) \quad \Rightarrow \quad g_0(g^* g \cdot (h \cdot h^* k))$$

$$= g_0(h \cdot (gg^* \cdot h^* k))$$

$$(3.3.2.2) \quad \Rightarrow \quad g_0(h \cdot (g \cdot g^* h^* k))t$$

$$= g_0(h \cdot (hg \cdot g^*)^* k)$$

$$= g_0((hg \cdot g^*)^* k \circ ht)$$

$$= (kt \circ (hg \cdot g^*)t) \circ ht$$

$$= (kt \circ ((ht \circ g) \circ ht)$$

$$= (kt \circ (g \circ ht \circ g)) \circ ht$$

$$= (z \circ (x \circ y \circ x)) \circ y.$$
Case 8a \(x, y, z \in Gt\), so let \(x = gt, y = ht, z = kt\). Thus

\[
(z \circ x) \circ (y \circ x \circ y) = (kt \circ gt) \circ (ht \circ gt \circ ht)
\]

\[
= g_0(g^*k \circ (ht \circ gt \circ ht))
\]

\[
= g_0g_0(g^*k \circ (g^*h \circ ht))
\]

\[
= g_0g_0(g^*k \circ (h \cdot g^*h)t)
\]

\[
= g_0g_0((h \cdot g^*h) \cdot g^*k)t
\]

\[
\text{(ARIF)} \quad = g_0g_0(h \cdot (g^*h^*)k)t
\]

\[
= g_0g_0(h \cdot (gh^*)^*k)t
\]

\[
= g_0g_0((gh^*)^*k \circ ht)
\]

\[
= g_0((kt \circ (g \cdot h^*)t) \circ ht)
\]

\[
= g_0((kt \circ (h^*g \circ gt)) \circ ht)
\]

\[
= (kt \circ (gt \circ ht \circ gt)) \circ ht
\]

\[
= (z \circ (x \circ y \circ x)) \circ y.
\]

Case 1b \(x, y, z \in G\). Then we are finished.

Case 2b \(x, y \in G\) and \(z \in Gt\), so let \(x = g, y = h, z = kt\). Thus

\[
(z \circ x) \circ (y \circ x \circ y) = (kt \circ g) \circ (h \circ g \circ h)
\]

\[
= (g^*k)t \circ (hgh)
\]

\[
= ((hgh)^*(g^*k))t
\]

\[
= ((h^*g^*h^*)(g^*k))t
\]

\[
\text{(ARIF)} \quad = (h^*(g^*h^*g^*)k)t
\]
Case 3b. $x, z \in G$ and $y \in Gt$, so let $x = g, y = ht, z = k$. Thus

\[(z \circ x) \circ (y \circ x \circ y) = (k \circ g) \circ (ht \circ g \circ ht) \]
\[= kg \circ (ht \circ (gh)t) \]
\[= g_0(kg \circ (h \cdot (gh)^*)) \]
\[= g_0(kg \cdot (h \cdot h^* g^*)) \]
\[= g_0((kg \cdot g^*) \cdot hh^*) \quad (3.3.2.1) \]
\[= g_0((k \cdot gg^*) \cdot hh^*) \]
\[= g_0((k \cdot hh^*) \cdot gg^*) \quad (3.3.2.1) \]
\[= g_0((kh \cdot h^*) \cdot gg^*) \]
\[= g_0(k(g^* g \cdot h) \cdot h^*) \quad (3.3.2.2) \]
\[= g_0(k(g^* \cdot gh) \cdot h^*) \]
\[= (kg^* h) \circ ht \]
\[= (k \circ (g^* \cdot gh) \circ ht) \]
\[= (k \circ ((gh) \circ ht) \circ g) \circ ht \]
\[= (k \circ (g \circ ht \circ g)) \circ ht \]

83
\[ (z \circ (x \circ y \circ x)) \circ y = (z \circ (x \circ y \circ x)) \circ y. \]

**Case 4b** Let \( y, z \in G \) and \( x \in Gt \), so let \( x = gt, y = h, z = k \). Thus

\[
(z \circ x) \circ (y \circ x \circ y) = (k \circ gt)(h \circ gt \circ h)
\]

\[
= (kg)t \circ (h \circ gt \circ h)
\]

\[
= (kg)t \circ ((hg)t \circ h)
\]

\[
= (kg)t \circ (h^* \cdot hg)t
\]

\[
= g_0(kg \cdot (h^* \cdot hg)^*)
\]

\[
= g_0(kg \cdot (g^* h^* \cdot h))
\]

\[
(3.3.2.1) \Rightarrow g_0(kg \cdot (g^* h^* h))
\]

\[
= g_0((kg \cdot g^*) \cdot h^* h)
\]

\[
(3.3.2.1) \Rightarrow g_0((k \cdot gg^*) \cdot h^* h)
\]

\[
= g_0((k \cdot h^* h) \cdot gg^*)
\]

\[
(3.3.2.1) \Rightarrow g_0((kh^* \cdot h) \cdot gg^*)
\]

\[
= g_0(k(h^* \cdot gg^*) \cdot h)
\]

\[
(3.3.2.1) \Rightarrow g_0(k(h^* g \cdot g^*) \cdot h)
\]

\[
= k((h^* g) \circ gt) \circ h
\]

\[
= (k \circ (gt \circ h \circ gt)) \circ h
\]

\[
= (z \circ (x \circ y \circ x)) \circ y.
\]
Case 5b $z \in G$ and $x, y \in Gt$, so let $x = gt, y = ht, z = k$. Thus

$$(z \circ x) \circ (y \circ x \circ y) = (k \circ gt) \circ (ht \circ gt \circ ht)$$

$$= (kg) t \circ (ht \circ gt \circ ht)$$

$$= g_0((kg) t \circ (hg^* \circ ht))$$

$$= g_0((kg) t \circ (hg^* \cdot h) t)$$

$$= g_0 g_0(kg \cdot (hg^* \cdot h)^*)$$

$$= g_0 g_0(kg \cdot (h^*gh^*)) \quad \text{(ARIF)}$$

$$= g_0 g_0(kg \cdot (h^*gh^*) t)$$

$$= g_0(kg \cdot (h^*g) t \circ ht)$$

$$= g_0(k \circ (gh^*g) t \circ ht)$$

$$= g_0(k \circ (gh^* \circ gt) \circ ht)$$

$$= (k \circ (gt \circ ht \circ gt)) \circ ht$$

$$= (z \circ (x \circ y \circ x)) \circ y.$$

Case 6b $x, z \in G$ and $y \in Gt$, so let $x = gt, y = h, z = k t$. Thus

$$(z \circ x) \circ (y \circ x \circ y) = (kt \circ gt) \circ (ht \circ gt \circ h)$$

$$= g_0(kg^* \circ (ht \circ gt \circ h))$$

$$= g_0(kg^* \circ ((hg) t \circ h))$$

$$= g_0(kg^* \circ (h^* \cdot hg) t)$$

$$= g_0(kg^* \cdot (h^* \cdot hg) t) \quad \text{[3.3.2.2]}$$

$$= g_0(kg^* \cdot (h^*h \cdot g)) t$$
\[= g_0((kg^*g) \cdot h^*h)t \]
\[(3.3.2.1) \Rightarrow g_0((k \cdot g^*g) \cdot h^*h)t \]
\[= g_0(g^*g \cdot (h^*h \cdot k))t \]
\[(3.3.2.2) \Rightarrow g_0(g^*g \cdot (h^*h \cdot k))t \]
\[= g_0(h^* \cdot (gg^*h)k)t \]
\[(3.3.2.2) \Rightarrow g_0(g^* \cdot (g \cdot g^*h)k)t \]
\[= g_0(h^* \cdot (h^*h \cdot g^*)k)t \]
\[= g_0(((h^*g \cdot g^*)k) \circ h) \]
\[= g_0((kt \circ (h^*g \cdot g^*)) \circ h) \]
\[= (kt \circ ((h^*g)t \circ gt)) \circ h \]
\[= (kt \circ (gt \circ h \circ gt)) \circ h \]
\[= (z \circ (x \circ y \circ x)) \circ y. \]

**Case 7b** \(x \in G\) and \(y, z \in Gt\), so let \(x = g, y = ht, z = kt\). Thus

\[(z \circ x) \circ (y \circ x \circ y) = (kt \circ g) \circ (ht \circ g \circ ht) \]
\[= (g^*k)t \circ (ht \circ g \circ ht) \]
\[= (g^*k)t \circ ((g^*h)t \circ ht) \]
\[= g_0((g^*k)t \circ (g^*h \cdot h^*)) \]
\[= g_0((g^*h \cdot h^*)^* \cdot g^*k)t \]
\[= g_0((h \cdot h^*g) \cdot g^*k)t \]
\[(3.3.2.2) \Rightarrow g_0((hh^* \cdot g) \cdot g^*k)t \]

586
\[= g_0(hh^* \cdot (g \cdot g^* k))t\]

\[\begin{aligned}
&\overset{(3.3.2.2)}{=} g_0(hh^* \cdot (gg^* \cdot k))t \\
&= g_0((k \cdot h^* h) \cdot g^* g)t \\
&\overset{(3.3.2.1)}{=} g_0((kh^* \cdot h) \cdot g^* g)t \\
&= g_0(k(h^* \cdot g^* g) \cdot h)t \\
&\overset{(3.3.2.1)}{=} g_0(k(h^* g^* g) \cdot h)t \\
&= g_0(k((gh)^* g) \cdot h)t \\
&= g_0(k(g^* gh)^* \cdot h)t \\
&= g_0(k(g^* gh)^* \circ ht) \\
&= (kt \circ (g^* gh)t) \circ ht \\
&= (kt \circ ((gh)t \circ g)) \circ ht \\
&= (kt \circ (g \circ ht \circ g)) \circ ht \\
&= (z \circ (x \circ y \circ x)) \circ y.
\end{aligned}\]

**Case 8b** \(x, y, z \in Gt\), so let \(x = gt, y = ht, z = kt\). Thus

\[\begin{aligned}
(z \circ x) \circ (y \circ x \circ y) &= (kt \circ gt) \circ (ht \circ gt \circ ht) \\
&= g_0(k^* \circ (ht \circ gt \circ ht)) \\
&= g_0 g_0(k^* \circ (hg^* \circ ht)) \\
&= g_0 g_0(k^* \circ (hg^* \cdot h)t) \\
&= g_0 g_0(k^* \cdot (hg^* \cdot h)t) \\
&\overset{(ARIF)}{=} g_0 g_0 (k(g^* hg^*)) \cdot h)t
\end{aligned}\]
Example 3.5.5. Let $G$ be the Symmetric Group on 3 letters, $S_3$. Define $g_0 = 1$ and $g^* = g^{-1}$ for all $g \in G$. Then $(G \cup Gt, \circ)$ with the multiplication in Theorem 3.3.5 gives a Moufang loop of order 12, the smallest example of a nonassociative Moufang loop. Moreover, $(G \cup Gt, \circ)$ with the multiplication in Theorem 3.3.6 gives a semiautomorphic IP loop of order 12, the smallest example that is non-Moufang and non-Steiner.

Flexible $C$-loops satisfy (ARIF) but not necessarily (RIF1) or (RIF2). Note that by Example 3.5.5, if $Q$ was a flexible $C$-loop, $(Q \cup Qt, \circ)$ isn’t necessarily a flexible $C$-loop. The following is an example showing that we cannot generalize Theorems 3.1.7 and 3.2.1 to flexible loops satisfying (ARIF).

Example 3.5.6. Let $(Q, \cdot)$ be a loop with multiplication given by the table below. Then $Q$ is a nonsemiautomorphic IP loop, flexible $C$-loop of order 20 were $R_{x,y}$ and $L_{x,y}$ are not semiautomorphisms and the commutant is not a subloop, found by MACE4 [37].

Example 3.5.7. Let $Q$ a commutative Moufang loop of order 81. Define $g_0 = 1$ and $g^* = g^{-1}$ for all $g \in G$. Then $(Q \cup Qt, \circ)$ with multiplication from Theorem 3.3.5 gives a semiautomorphic IP loop where $N(Q) \nsubseteq Q$. 

\[= g_0g_0(k(gh^* \cdot g)^* \cdot h)t\]
\[= g_0g_0(k(gh^* \cdot g)^* \circ ht)\]
\[= g_0((kt \circ (gh^* \cdot g)t) \circ ht)\]
\[= g_0((kt \circ (gh^* \circ gt)) \circ ht)\]
\[= (kt \circ (gt \circ ht \circ gt)) \circ ht\]
\[= (z \circ (x \circ y \circ x)) \circ y. \]
|  1 |  2 |  3 |  4 |  5 |  6 |  7 |  8 |  9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|  2 |  4 |  1 |  3 |  7 |  8 |  6 |  5 | 10 |  9 | 11 | 19 | 20 | 17 | 18 | 16 | 15 | 14 | 13 | 12 |
|  3 |  1 |  4 |  2 |  8 |  7 |  5 |  6 | 11 |  9 | 12 | 10 | 20 | 19 | 18 | 17 | 15 | 16 | 13 | 14 |
|  4 |  3 |  2 |  1 |  6 |  5 |  8 |  7 | 12 | 11 | 10 |  9 | 14 | 13 | 16 | 15 | 18 | 17 | 20 | 19 |
|  5 |  7 |  8 |  6 |  4 |  1 |  3 |  2 | 13 | 17 | 18 | 14 | 12 |  9 | 19 | 20 | 11 | 10 | 16 | 15 |
|  6 |  8 |  7 |  5 |  1 |  4 |  2 |  3 | 14 | 18 | 17 | 13 |  9 | 12 | 20 | 19 | 10 | 11 | 15 | 16 |
|  7 |  6 |  5 |  8 |  3 |  2 |  1 |  4 | 15 | 19 | 20 | 16 | 17 | 18 |  9 | 12 | 13 | 14 | 10 | 11 |
|  8 |  5 |  6 |  7 |  2 |  3 |  4 |  1 | 16 | 20 | 19 | 15 | 18 | 17 | 12 |  9 | 14 | 13 | 11 | 10 |
|  9 |  10 | 11 | 12 | 13 | 14 | 16 | 15 |  1 |  2 |  3 |  4 |  5 |  6 |  8 |  7 | 19 | 20 | 17 | 18 |
|  10 | 12 |  9 | 11 | 17 | 18 | 20 | 19 |  2 |  4 |  1 |  3 | 16 | 15 | 13 | 14 |  6 |  5 |  7 |  8 |
|  11 |  9 | 12 | 10 | 18 | 17 | 19 | 20 |  3 |  1 |  4 |  2 | 15 | 16 | 14 | 13 |  5 |  6 |  8 |  7 |
|  12 | 11 | 10 |  9 | 14 | 13 | 15 | 16 |  4 |  3 |  2 |  1 |  6 |  5 |  7 |  8 | 20 | 19 | 18 | 17 |
|  13 | 19 | 20 | 14 | 12 |  9 | 18 | 17 |  5 | 15 | 16 |  6 |  4 |  1 | 11 | 10 |  7 |  8 |  3 |  2 |
|  14 | 20 | 19 | 13 |  9 | 12 | 17 | 18 |  6 | 16 | 15 |  5 |  1 |  4 | 10 | 11 |  8 |  7 |  2 |  3 |
|  15 | 17 | 18 | 16 | 19 | 20 | 12 |  9 |  7 | 14 | 13 |  8 | 10 | 11 |  4 |  1 |  3 |  2 |  6 |  5 |
|  16 | 18 | 17 | 15 | 20 | 19 |  9 | 12 |  8 | 13 | 14 |  7 | 11 | 10 |  1 |  4 |  2 |  3 |  5 |  6 |
|  17 | 16 | 15 | 18 | 11 | 10 | 14 | 13 |  9 |  6 |  5 | 20 |  8 |  7 |  3 |  2 |  1 |  4 |  9 | 12 |
|  18 | 15 | 16 | 17 | 10 | 11 | 13 | 14 |  20 |  5 |  6 | 19 |  7 |  8 |  2 |  3 |  4 |  1 | 12 |  9 |
|  19 |  9 | 14 | 13 | 20 | 16 | 15 | 11 | 10 | 17 |  8 |  7 | 18 |  3 |  2 |  6 |  5 |  9 | 12 |  1 |
|  20 | 13 | 14 | 19 | 15 | 16 | 10 | 11 | 18 |  7 |  8 | 17 |  2 |  3 |  5 |  6 | 12 |  9 |  4 |  1 |

Table 3.4: A non-semiautomorphic flexible C-loop
Chapter 4

Simple Right Conjugacy Closed Loops

Most of the literature on the one-sided conjugacy closed loops deals with left conjugacy closed loops [3, 13, 14, 41]. RCC loops are the more natural choice here since our permutations act on the right.

For (two-sided) CC-loops, the existence of nonassociative simple loops is settled in the negative by Basarab’s Theorem [3]: The factor of a CC-loop by its (necessarily normal) nucleus is an abelian group. It follows that a simple CC-loop must have nucleus coinciding with the whole loop, hence is a group.

In the one-sided case, nonassociative simple RCC loops are known to exist. The first example occurring in the literature seems to be the simple Bol loop of exponent 2 and order 96 constructed by G. Nagy [39], because a right Bol loop of exponent 2 is necessarily an RCC loop. Other examples arose in the computer search for nonassociative, finite simple automorphic loops [28].

In this chapter we give the first general construction of a large class of nonas-
sociative, finite simple RCC loops. Our construction by no means accounts for all such loops; for example, Nagy’s Bol loop of exponent 2 does not fit this construction. Thus a full classification of finite simple RCC loops is still elusive. Nevertheless, we have found by exhaustive computer search that our construction accounts for all finite simple RCC loops up to order 15.

4.1 Right Conjugacy Closed loops

**Proposition 4.1.1.** For a loop $Q$, the following are equivalent:

1. $Q$ is an RCC loop,

2. The following holds for all $x, y, z \in Q$:

   \[ R^{-1}_x R_y R_x = R_{x \setminus yx}. \]  \hfill (RCC$_1$)

3. The following holds for all $x, y, z \in Q$:

   \[ (xy)z = (xz) \cdot z \setminus (yz). \]  \hfill (RCC$_2$)

4. For all $x \in Q$, $(R_a, R_a L_a^{-1}, R_a) \in \text{Atp}(Q)$.

**Proof.** If $Q$ is an RCC loop, then $\forall x, y \in Q$, we have $R_x^{-1} R_y R_x = R_z \iff R_y R_x = R_z$. Hence, applying this to 1 gives $yx = xz$, and thus, $z = x \setminus yx$. Similarly, (RCC$_1$) holds if and only if $R_y R_z = R_z R_{z \setminus yz}$ for all $y, z \in Q$, which is clearly equivalent to (RCC$_2$). Finally, $(R_a, R_a L_a^{-1}, R_a) \in \text{Atp}(Q)$ is simply (RCC$_2$). \[\square\]

**Proposition 4.1.2.** Let $Q$ be a RCC loop. Then
\[(i) \quad N_\mu(Q) = N_\rho(Q) \trianglelefteq Q \quad \text{and} \]
\[(ii) \quad C(Q) \leq N_\lambda(Q). \]

**Proof.** For (i), note that
\[(id_Q, R_a, R_a) (R_a, L_a^{-1}, id_Q) = (R_a, R_a L_a^{-1}, R_a) \in \text{Atp}(Q).\]

Therefore, if \((id_Q, R_a, R_a)\) or \((R_a, L_a^{-1}, id_Q)\) is in \(\text{Atp}(Q)\), the other one is as well.

For normality, see [13].

For (ii), let \(a \in C(Q)\). Then, using (RCC\(_2\)), we have
\[ax \cdot y = xa \cdot y = xy \cdot y \setminus (ay) = xy \cdot a = a \cdot xy. \]

Our goal is to construct simple RCC loops. Therefore, it is vital to understand the structure of normal subloops of an RCC loop. Let \(Q\) be a RCC-loop with \(N \trianglelefteq Q\) and consider \(R_N = \{R_x \mid x \in N\}\). Fix \(x \in N\) and then \(\forall y \in Q, R_y R_x R_y^{-1} = R_{yx/y} \in R_N\) since \(yx/y \in N\). Hence, normal subloops of \(Q\) correspond to unions of conjugacy classes in \(R_Q\).

### 4.2 Constructing Simple RCC loops

Let \(\mathbb{F}_q\) be the finite field of order where \(q = p^n\) for a prime \(p\) and some \(n > 0\).

For a matrix \(M\), let \(\text{Det}(M)\) denote the **determinant of the matrix** \(M\), \(\text{Tr}(M)\) denote the **trace of the matrix** \(M\) and \(\text{Char}(M)\) denote the **characteristic polynomial of the matrix** \(M\). All matrices will be of size \(2 \times 2\) (**i.e.** \(M \in GL(2,q)\)), hence \(\text{Char}(M) = x^2 - Tr(M)x + Det(M) \in \mathbb{F}_q[x]\).
First, let \( f(x) = x^2 - rx + s \) be irreducible in \( \mathbb{F}_q[x] \). For each \( b \in \mathbb{F}_q \), define

\[
M_{(0,b)} = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}
\]

and for \( a \neq 0 \),

\[
M_{(a,b)} = \begin{pmatrix} r - b & f(b) \\ -a & a b \end{pmatrix}.
\]

Note that \( \text{Det}(M_{(a,b)}) = s \) and \( \text{Tr}(M_{(a,b)}) = r \) and thus \( \text{Char}(M_{(a,b)}) = f(x) \).

**Lemma 4.2.1.** Let \( f(x) = x^2 - rx + s \) be irreducible in \( \mathbb{F}_q[x] \). The conjugacy class of all matrices in \( GL(2,q) \) with characteristic polynomial \( f(x) \) is precisely the set \( \{M_{(a,b)} \mid a, b \in \mathbb{F}_q \} \) for \( a \neq 0 \).

**Proof.** Note that if two elements of \( GL(2,q) \) are conjugate then they both have the same characteristic polynomial, and hence for a \( 2 \times 2 \) matrix, have the same determinant and trace [46]. Now suppose \( M = \begin{pmatrix} c & d \\ a & b \end{pmatrix} \) has \( \text{Char}(M) = f(x) \). Note that \( a \neq 0 \) since \( f(x) \) is irreducible; otherwise, \( M \) would have \( c \) and \( b \) as eigenvalues. Now \( r = \text{Tr}(M) = c + b \), so that \( c = r - b \). Also, \( s = \text{Det}(M) = (r - b)b - da \), and so \( -da = b^2 - rb + s = f(b) \). Hence \( d = f(b)/(-a) \). Therefore \( M = M_{(a,b)} \) as claimed.

Let \( f(x) = x^2 - rx + s \) be irreducible in \( \mathbb{F}_q[x] \). Let \( Q = \mathbb{F}_q^2 \setminus \{(0,0)\} \), written as a set of row vectors. Define a binary operation \( \circ_f \) on \( Q \) by

\[
[a,b] \circ_f [c,d] = [a,b]M_{(c,d)}.
\]
Note that
\[
[a, b] \circ_f [c, d] = [a(r - d) + bc, \frac{-af(d)}{c} + bd] \quad c \neq 0,
\]
\[
[a, b] \circ_f [c, d] = [ad, bd] \quad c = 0.
\]

It is clear that $\circ_f$ is closed on $Q$. Indeed, if $[a, b] \circ_f [c, d] = [0, 0]$ and $c = 0$, then either both $a = b = 0$ or $d = 0$.

For $c \neq 0$, if $d = 0$, then $ar + bc = -\frac{as}{c} = 0$. Thus, either $a = 0$ implying $b = 0$ or $s = 0$. For $d \neq 0$, we have
\[
r - d = \frac{-bc}{a} = -d + r - s = d
\]
implying $s = 0$. Therefore, $[a, b] \circ_f [c, d] = [0, 0]$ if and only if either $[a, b] = [0, 0]$ or $[c, d] = [0, 0]$.

**Remark 4.2.2.** To keep notation clear; $[x, y]$ denotes an element in $Q$; $R_{[x, y]}$ denotes the right translation by $[x, y]$; and $M_{(x, y)}$ denotes the matrix associated with the right translation by $[x, y]$.

**Theorem 4.2.3.** $(Q, \circ_f)$ is a loop.

**Proof.** First note that $R_{(Q, \circ_f)} = \{M(a, b) \mid a, b \in F_q\} \setminus \{M(0, 0)\}$ by the definition of $\circ_f$.

That is, $R_{[a, b]}$ corresponds uniquely to $M_{(a, b)}$ by construction. Now, by Proposition 1.1.1, it is enough to show that each $R_{[y, z]}M_{(u, v)}^{-1}$ is fixed-point free.

Let $M_{(y, z)}, M_{(u, v)} \in R_{(Q, \circ_f)}$ and suppose $M_{(y, z)}M_{(u, v)}^{-1}$ has a fixed point. Then, $M_{(y, z)}M_{(u, v)}^{-1}$ has an eigenvalue of 1. Let $g(x) = \text{Char}(M_{(y, z)}M_{(u, v)}^{-1})$. Then
\[
g(x) = x^2 - Tr(M_{(y, z)}M_{(u, v)}^{-1})x + Det(M_{(y, z)}M_{(u, v)}^{-1}),
\]
94
\[ 0 = g(1) = 1^2 - Tr(M_{(y,z)}M_{(u,v)}^{-1}) + Det(M_{(y,z)}M_{(u,v)}^{-1}) \]
\[ = 1 - Tr(M_{(y,z)}M_{(u,v)}^{-1}) + 1. \]

Thus, \( Tr(M_{(y,z)}M_{(u,v)}^{-1}) = 2 \). Therefore, \( g(x) = x^2 - 2x + 1 = (x - 1)^2 \). Then, either \( M_{(y,z)}M_{(u,v)}^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \) or \( M_{(y,z)}M_{(u,v)}^{-1} \) is similar to \( \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \). In the first case, we have \( M_{(y,z)} = M_{(u,v)} \). For the second, suppose \( M_{(y,z)} \neq M_{(u,v)} \) and let \( P \in GL(2, q) \) such that \( PM_{(y,z)}M_{(u,v)}^{-1}P^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \). Then define \( A = PM_{(y,z)}P^{-1} \) and \( B = PM_{(u,v)}P^{-1} \), so that \( AB^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \). Note that \( A \) and \( B \) have the same determinant and trace as \( M_{(y,z)} \) and \( M_{(u,v)} \), respectively and hence \( Char(A) = Char(B) = f(x) \). Let \( A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, B = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \). Then \( [1, 0]A = [1, 1]B \) and \( [0, 1]A = [0, 1]B \).

Hence \( a = e + g, b = f + h, c = g, d = h \). Thus \( A = \begin{pmatrix} e + g & f + h \\ g & h \end{pmatrix} \) and since \( Tr(A) = Tr(B), g = 0 \). Hence, \( A, B \) are upper triangular matrices and therefore \( Char(A) = f(x) \) is reducible, which is a contradiction. \( \square \)

**Lemma 4.2.4.** In \((Q, \circ f)\)

(i) for \( a \neq 0 , R_{[a,b]}^{-1} = M_{(a,b)}^{-1} = \begin{pmatrix} r - b & f(b) \\ a & b \end{pmatrix}^{-1} = \frac{1}{s} \begin{pmatrix} b & f(b)/a \\ -a & r - b \end{pmatrix} = \frac{1}{s} M_{[-a, r-b]}, \)

(ii) \( R_{[0,b]} = \frac{1}{b} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \),

95
(iii) \( R_{[a,b],[c,d]} = M_{(a,b)}M_{(c,d)}M_{[a,b] \circ [c,d]}^{-1} = \left( \begin{array}{cc} s & -(a^2 s f(d) -abcds -abcd + aber + acdr - acrs + acr^2 + abcr + acdr - acr^2 + acrs + c^2 f(b)) \\ 0 & 1 \end{array} \right) \)

(iv) \( R_{[a,b],[0,d]} = M_{(a,b)}M_{(0,d)}M_{[a,b] \circ [0,d]}^{-1} = \left( \begin{array}{cc} d^2 & \frac{(d-1)(b-r+bd)}{a} \\ 0 & 1 \end{array} \right) \)

(v) \( R_{[0,b],[c,d]} = M_{(0,b)}M_{(c,d)}M_{[0,b] \circ [c,d]}^{-1} = \left( \begin{array}{cc} b^2 & \frac{(b-1)(d-r+bd)}{c} \\ 0 & 1 \end{array} \right) \) and

(vi) \( R_{[0,b],[0,d]} = M_{(0,b)}M_{(0,d)}M_{[0,b] \circ [0,d]}^{-1} = \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) \).

Proof. For (i), simply note

\[
[x,y] \left( \begin{array}{cc} r - b & \frac{f(b)}{-a} \\ a & b \end{array} \right) \left( \begin{array}{cc} r - b & \frac{f(b)}{-a} \\ a & b \end{array} \right)^{-1} = [x(r-b)+ay, \frac{-x(f(b))}{c}] + by \left( \begin{array}{cc} b \frac{f(b)}{sa} \\ \frac{-a}{s} \frac{f(b)}{sa} \end{array} \right) = [x,y].
\]

Similarly, for (ii). For (iii), using (i), we have

\[
M_{(a,b) \circ [c,d]}^{-1} = \left( \begin{array}{cc} \frac{-(a\alpha f(d)+bd)}{c} & \frac{f(-a\alpha f(d)+bd)}{sa} \\ \frac{-a}{s} \frac{f(-a\alpha f(d)+bd)}{sa} & \frac{r-(a\alpha f(d)+bd)}{s} \end{array} \right).
\]
Therefore, we have

\[
\begin{pmatrix}
  r - b & -f(b) \\
  a & b
\end{pmatrix} \begin{pmatrix}
  r - d & -f(d) \\
  c & d
\end{pmatrix} \begin{pmatrix}
  \frac{-as d}{s} + bd & \frac{f(-as d)}{s} \\
  - (a(r-d)+bc) & \frac{r - (as d)}{s}
\end{pmatrix} = \begin{pmatrix}
  s & -\frac{(a^2 sf(d) - abcd - abed + abcr + acdr - acrs + c^2 f(b))}{(ac (bc - ad + ar))} \\
  0 & 1
\end{pmatrix}.
\]

A similar calculation gives (iv). Finally, (v) and (vi) follow from (iv) and Lemma 1.1.3.

It is well known that the center of $GL(n, q)$ are scalar multiples of $I$ [46]. Thus, we have the following:

**Lemma 4.2.5.** $C(Q, \circ f) = \{[0, b] | \forall b \in \mathbb{F}_q b \neq 0\}$. That is, the only elements of $C(Q, \circ f)$ are in the set $\{R_{[a, b]} | [a, b] \in C(Q, \circ f)\}$.

**Proof.** Using Propositions 1.1.3, 4.1.2 and the above remark, we are done.

Now, the loop $(Q, \circ f)$ has been constructed such that $R_{(Q, \circ f)}$ is a union of conjugacy classes in $GL(2, q)$, namely the center $Z(GL(2, q))$ (scalar matrices) and the conjugacy class of matrices $M$ with $Char(M) = f(x)$.

**Theorem 4.2.6.** $(Q, \circ f)$ is an RCC loop.

**Proof.** Let $[a, b] \in (Q, \circ f)$ . First, if $a = 0$ then, $M_{(0, b)} = \begin{pmatrix}
  b & 0 \\
  0 & b
\end{pmatrix}$ and

$$[0, b] \in C(Q, \circ) \cap N_\lambda (Q, \circ) \Rightarrow R_{(0, b)} \in Z(Mlt_p (Q, \circ))$$
by Proposition 1.1.3 and Lemma 4.2.5. Therefore, for any \([c, d] \in (\mathbb{Q}, \circ)\),

\[
R_{[c,d]}R_{[0,b]}R^{-1}_{[c,d]} = M_{(c,d)}M_{(0,b)}M^{-1}_{(c,d)} = M_{(c,d)}M^{-1}_{(c,d)}M_{(0,b)} = M_{(0,b)} = R_{[0,b]}.
\]

Else, let \([c, d] \in (\mathbb{Q}, \circ)\) and see that

\[
\text{Det}(M_{(c,d)}M_{(a,b)}M^{-1}_{(c,d)}) = \text{Det}(M_{(a,b)})\text{Det}(M_{(c,d)}) = sss^{-1} = s = \text{Det}(M_{(a,b)}).
\]

Similarly, \(Tr(M_{(c,d)}M_{(a,b)}M^{-1}_{(c,d)}) = r\). Hence \(R_{[c,d]}R_{[a,b]}R^{-1}_{[c,d]} \in R_{(\mathbb{Q}, \circ)}\).

**Lemma 4.2.7.** Let \(q \neq 3\). Then \(C(\mathbb{Q}, \circ_f) = N_{\lambda}(\mathbb{Q}, \circ_f)\). If \(q = 3\) and \(r \neq 0\), then 
\(C(\mathbb{Q}, \circ_f) = N_{\lambda}(\mathbb{Q}, \circ_f)\).

**Proof.** For \(q = 2\), \(|(\mathbb{Q}, \circ_f)| = 3\), and is an abelian group. Let \(q > 3\) and note that there exists a \(d \in \mathbb{F}_q\) such that \(d^2 \neq 1\). Suppose \([x, y] \in N_{\lambda}(\mathbb{Q}, \circ_f)\). Then for any \(a \in \mathbb{F}_q \setminus \{0\},\)

\[
([x, y] \circ_f [a, 0]) \circ_f [0, d] = [x, y] \circ_f ([a, 0] \circ_f [0, d]),
\]

or equivalently, \([x, y]R_{[a, 0]}, [0, d] = [x, y]\). Hence, by Proposition 4.2.4(iv), \(d^2 x = x\).

But \(d^2 \neq 1\), and thus we have \(x = 0\). When \(q = 3\) and \(r = 0\), \(C(\mathbb{Q}, \circ_f) < N_{\lambda}(\mathbb{Q}, \circ_f)\).

Finally, for \(r \neq 0\), let \(d \neq 1\). Then, as before, Proposition 4.2.4(iv) gives

\[
y - \frac{rx(d - 1)}{a} = y.
\]

But \(r \neq 0\) and hence, \(x = 0\). \(\square\)
As noted before, normal subloops of $Q$ correspond to unions of conjugacy classes of matrices in $GL(2,q)$ which are contained in $R(\circ f)$. $R(\circ f)$ itself is the union of conjugacy classes, namely, $\{M(a,b)\mid a, b \in Q, a, b \neq 0\}$, which has size $q^2 - q$, and the $q - 1$ one-element conjugacy classes in the center of $GL(2,q)$. Since the order of a normal subloop of $Q$ must divide $|Q| = q^2 - 1$, we have the following.

**Lemma 4.2.8.** The only non-trivial normal subgroups of $(Q, \circ f)$ are $C(Q, \circ f)$ and $\{[0, 1], [0, -1]\}$.

**Proof.** Using the above remark, the only options are matrices of the form
$$\begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}.$$ Hence, either we have the $C(Q, \circ f)$ or $\{[0, 1], [0, -1]\} \leq C(Q, \circ f)$. \hfill \qed

**Theorem 4.2.9.** Let $f(x) = x^2 - rx + s$ be irreducible. If $r \neq 0$, then $(Q, \circ f)$ is simple. If $r = 0$, then $Z(Q, \circ f) = \{[0, \pm 1]\}$ and $(Q, \circ f)/Z(Q, \circ f)$ is simple.

**Proof.** Let $Tr(M_{a,b}) \neq 0$ and suppose $(N, \circ f) \triangleleft (Q, \circ f)$. Then, by Lemma 4.2.7, $(N, \circ f) \leq C(Q, \circ f) = N_1(Q, \circ f)$. Fix $[0, z] \in (N, \circ f)$ and let $[0, a], [0, c] \in (Q, \circ f)$. Then
$$[c, 0] \circ f ([a, 0] \circ f [0, z]) = ([c, 0] \circ f [a, 0]) \circ f [0, z].$$ Thus, $[cr, \frac{-cz}{a}] = [cz, \frac{-cz}{a}]$. Hence $z = 1$. That is, if
$$(N, \circ f) \triangleleft (Q, \circ f) \iff (N, \circ f) = \{[0, 1]\}.$$ Therefore, the only normal subloops are trivial and $(Q, \circ f)$ is simple.
Else, let \([a, b], [c, d] \in (\mathbb{Q}, \circ_f)\) and \([0, z] \in (N, \circ_f)\). Note that

\[
M(a, b) = \begin{pmatrix} -b & \frac{s + b^2}{-a} \\ a & b \end{pmatrix}, \quad M(c, d) = \begin{pmatrix} -d & \frac{s + d^2}{c} \\ c & d \end{pmatrix}.
\]

Now,

\[
[c, d] \circ_f ([a, b] \circ_f [0, z]) = ([c, d] \circ_f [a, b]) \circ_f [0, z].
\]

implies

\[
[z(ad - bc), bdz - \frac{c(b^2z^2 + s)}{az}] = [z(ad - bc), z(bd - \frac{c(b^2 + s)}{a})].
\]

This is only solvable when \(z = \pm 1\), and hence, \(Z(\mathbb{Q}, \circ_f) = \{[0, \pm 1]\}\). Therefore, \((\mathbb{Q}, \circ_f)\) is not simple. However, \((\mathbb{Q}, \circ_f)/Z(\mathbb{Q}, \circ_f)\) is simple, since our same computation would for \(z = \pm 1\) in \((\mathbb{Q}, \circ_f)/Z(\mathbb{Q}, \circ_f)\), but \([0, 1] = [0, -1]\) in this loop. Thus, the only possible normal subloops are again trivial. \(\Box\)

### 4.3 Conclusion

The following is an example for constructing a simple RCC loop of order 8, from \(GL(2, 3)\).

**Example 4.3.1.** Let \(q = 3\) and hence the elements of \((\mathbb{Q}, \circ_f)\) are

\[
\{1 = [0, 1], 2 = [0, 2], 3 = [1, 0], 4 = [1, 1], 5 = [1, 2], 6 = [2, 0], 7 = [2, 1], 8 = [2, 2]\}.
\]

Let \(f(x) = x^2 + 2x + 2\) be irreducible in \(\mathbb{F}_3\). Then conjugacy class of all matrices in
$GL(2, 3)$ with characteristic polynomial $f(x)$ are

$$\left\{ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} \right\}.$$ 

Hence, the full set of matrices are

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix} \right\},$$

so that

$$M_{(0, 1)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, M_{(0, 2)} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, M_{(1, 0)} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \ldots$$

Now, act on elements in $(Q, \circ f)$ by the matrices above, giving the permutations for $R_{(Q, \circ f)}$. For example, $M_{(2, 2)} = \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}$ gives the permutation $(1, 8, 6, 5, 2, 4, 3, 7)$ because

\[
\begin{align*}
[0, 1] \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} &= [2, 2], \\
[0, 2] \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} &= [1, 1], \\
[1, 0] \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} &= [2, 1], \\
[1, 1] \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} &= [2, 1], \\
[1, 2] \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} &= [0, 2], \\
[2, 0] \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} &= [1, 2], \\
[2, 1] \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} &= [0, 1], \\
[2, 2] \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} &= [2, 0].
\end{align*}
\]
Hence, we have

\[ R(Q, \circ f) = \{(), (1,2)(3,6)(4,8)(5,7), (1,3,4,7,2,6,8,5), (1,4,5,6,2,8,7,3), \]
\[ (1,5,3,8,2,7,6,4), (1,6,7,4,2,3,5,8), (1,7,8,3,2,5,4,6), \]
\[ (1,8,6,5,2,4,3,7) \}. \]

Since \( r \neq 0 \), \((Q, \circ f)\) is simple and has the following multiplication table.

\[
\begin{array}{c|cccccccc}
\circ f & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
\hline
1 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
2 & 2 & 1 & 6 & 8 & 7 & 3 & 5 & 4 \\
3 & 3 & 6 & 4 & 1 & 8 & 5 & 2 & 7 \\
4 & 4 & 8 & 7 & 5 & 1 & 2 & 6 & 3 \\
5 & 5 & 7 & 1 & 6 & 3 & 8 & 4 & 2 \\
6 & 6 & 3 & 8 & 2 & 4 & 7 & 1 & 5 \\
7 & 7 & 5 & 2 & 3 & 6 & 4 & 8 & 1 \\
8 & 8 & 4 & 5 & 7 & 2 & 1 & 3 & 6 \\
\end{array}
\]

Table 4.1: Multiplication Table for \((Q, \circ f)\)

We now consider two questions:

1. What group is \(\text{Mlt}_\rho(Q, \circ f)\)?

2. How many nonisomorphic RCC loops can be made from \(GL(2,q)\)?

For (1), we have \(\text{Mlt}_\rho(Q) = \text{Inn}_\rho(Q) \cdot R_Q\). Indeed, for \(\theta \in \text{Mlt}_\rho(Q)\) set \(a = 1\). Then \(\psi = \theta R_a^{-1}\) fixes 1, hence is an element of \(\text{Inn}_\rho(Q)\). Therefore, \(\theta = \psi R_a\) and since \(\text{Inn}_\rho(Q) \cap R_Q = \mathbb{1}\), we have the factorization.

**Conjecture 1.** \(\text{Inn}_\rho(Q, \circ f) = \{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} | x = a^2 s^m, a, y \in \mathbb{F}_q, m \in \mathbb{Z} \}.\)
We know $x$ must have this form from Lemma 4.2.4. The question is whether we can have any value for $y \in \mathbb{F}_q$. We do have the following.

**Lemma 4.3.2.** Let $H = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \mid x, y \in \mathbb{F}_q \right\}$. Then $GL(2, q) = R(Q, \circ f) \cdot H$.

**Proof.** Note that $|R(Q, \circ f)| = q^2 - 1$ and $|H| = q(q - 1)$. We have $|GL(2, q)| = (q^2 - 1)(q^2 - q) = q(q + 1)(q - 1)^2 = |R_Q||H|$. Since $R(Q, \circ f) \cap H = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, we have the desired result. \qed

Hence, question (1) reduces to what subgroups of $H$ can occur as $\text{Inn}_p(Q, \circ f)$?

For question (2), there are $\frac{q^2 - q}{2}$ irreducible polynomials of degree 2 over $\mathbb{F}_q$. Hence, one would think that we would create the same number of nonisomorphic RCC loops for a given $q$. This is not true, however. For example, when $q = 4$, there are 6 irreducible polynomials over $\mathbb{F}_4$ and we create 6 RCC loops associated to each polynomial. However, only 3 are nonisomorphic, and each is simple. For $q = 8$, we have only 10 nonisomorphic RCC loops, instead of 28 we can construct. However, when $q$ is a prime, we seem have a one-to-one correspondence on the number of nonisomorphic RCC loops and the number of irreducible polynomials over $\mathbb{F}_q$.

**Conjecture 2.** Let $p$ be a prime number.

1. If $q = p$, then the number of nonisomorphic RCC loops constructed from $GL(2, q)$ is $\frac{q^2 - q}{2}$.

2. If $q = p^2$, then the number of nonisomorphic RCC loops constructed from $GL(2, q)$ is $\frac{q^2 - q}{4}$. 

103
The following table gives a count of RCC loops constructed from $GL(2,q)$. Note that RCC loops of order $p$ a prime are groups [13]. Our list is complete for simple RCC loops up to and including order 15. That is, there is no simple RCC loop of order 15 or less that is not counted in this list. Also, for the loops of order 24, 10 loops are constructed from $GL(2,5)$ and 3 are constructed from $GL(2,7)$.

<table>
<thead>
<tr>
<th>$q$</th>
<th>Order</th>
<th>Number of primitive polynomials</th>
<th>Number of non-isomorphic, nonassociative RCC Loops</th>
<th>Number of Simple RCC loops</th>
<th>Exhaustive</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>8</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>✓</td>
</tr>
<tr>
<td>5</td>
<td>12</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>✓</td>
</tr>
<tr>
<td>4</td>
<td>15</td>
<td>6</td>
<td>3</td>
<td>3</td>
<td>✓</td>
</tr>
<tr>
<td>5,7</td>
<td>24</td>
<td>10,3</td>
<td>13</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>40</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>48</td>
<td>21</td>
<td>21</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>60</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>63</td>
<td>28</td>
<td>10</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>80</td>
<td>36</td>
<td>18</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>84</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>120</td>
<td>55</td>
<td>55</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>168</td>
<td>78</td>
<td>78</td>
<td>72</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>255</td>
<td>120</td>
<td>30</td>
<td>30</td>
<td></td>
</tr>
</tbody>
</table>

Table 4.2: Table of RCC Loops
Chapter 5

Pseudoautomorphisms of Bruck loops and their generalizations

Bruck loops are the motivation for our main result in this section, but we will state and prove it in much more generality (hence the generalizations mentioned in the title). The class of loops we will consider are those with two-sided inverses such that (WIP) holds. These were introduced by Johnson and Sharma [29] who called them weak commutative inverse property loops (WCIP loops). It is clear that any loop with the RIP and AIP satisfies WCIP. This applies in particular to (right) Bruck loops or even to the more general class of Kikkawa loops [30]. In fact, it is evident that any two of the properties RIP, AIP and WCIP imply the third. This chapter is joint work with M.K. Kinyon.
5.1 Weak commutative inverse property loops

Lemma 5.1.1. A loop $Q$ has the WCIP if and only if for all $x, y \in Q$,

$$y^{-1} \cdot x^{-1} = x \cdot y$$

(WCIP2)

Proof. Replacing $y$ in (WCIP) with $x \cdot y$ and rearranging, we obtain (WCIP2). Replacing $y$ in (WCIP2) with $xy$ and rearranging, we obtain (WCIP). \qed

In particular, Lemma 5.1.1 shows that a loop $Q$ has the WCIP if and only if the isotrophic loop $[42] (Q, \circ)$ defined by $x \circ y = x^{-1} \cdot y$ is commutative.

Before turning to our main result, we will show that in the present setting we can dispense with the notion of middle pseudoautomorphism. In a loop $Q$ with two-sided inverses, we will denote the inversion map by $J : Q \to Q; x \mapsto x^{-1}$.

Lemma 5.1.2. Let $Q$ be loop with WCIP. If $(\alpha, \beta, \gamma) \in \text{Atp}(Q)$, then

$$(J \gamma J, \beta, J \alpha J) \in \text{Atp}(Q).$$

Proof. Since $(\alpha, \beta, \gamma) \in \text{Atp}(Q)$, we have $x \alpha \cdot y \beta = (xy) \gamma$ for all $x, y \in Q$. Thus

$$(xy) \gamma J \cdot y \beta = (x \alpha \cdot y \beta)J \cdot y \beta = x \alpha J$$

using the WCIP. Replace $x$ with $(xy)^{-1}$ and use the WCIP again to get $x J \gamma J \cdot y \beta = (xy) J \alpha J$ for all $x, y \in Q$. Thus $(J \gamma J, \beta, J \alpha J) \in \text{Atp}(Q).$ \qed

Lemma 5.1.3. Let $Q$ be a loop with WCIP and let $\sigma \in \text{Sym}(Q)$. Then $\sigma$ is a middle pseudoautomorphism with companion $c$ if and only if $J \sigma J$ is a right pseudoautomorphism with companion $c^{-1}$.

Proof. Suppose $\sigma$ is a middle pseudoautomorphism with companion $c$ so that

$$(\sigma R_{c^{-1}}, \sigma L_{c^{-1}}, \sigma)$$

is an autotopism. By Lemma 5.1.2, $(J \sigma J, \sigma L_{c^{-1}}, J \sigma R_{c^{-1}} J) \in \text{Atp}(Q)$. \qed
Atp($Q$). Since the first component fixes 1, this autotopism lies in Atp$_\rho(Q)$, and so the second and third components coincide and have the form $J\sigma JR_c$ for some $d$. To determine $d$, we compute $d = 1J\sigma R^{-1}_cJ = c^{-1}$. Thus $(J\sigma J, J\sigma JR_c, J\sigma JR_c) \in$ Atp$_\rho(Q)$, that is, $\sigma$ is a right pseudoautomorphism with companion $c^{-1}$. The converse is similar. 

As an aside, we mention that a similar result holds for loops with the right inverse property: $\sigma$ is a middle pseudoautomorphism with companion $c$ if and only if $\sigma$ is a right pseudoautomorphism with companion $c$. In place of Lemma 5.1.2, the argument uses the fact that in RIP loops, $(\alpha, \beta, \gamma) \in$ Atp($Q$) implies $(\gamma, J\beta J, \alpha) \in$ Atp($Q$) [30].

As a corollary of Lemmas 1.1.4 and 5.1.3, we re-obtain a fact from [29].

**Corollary 5.1.4.** In a loop $Q$ with WCIP, $N_\mu(Q) = N_\rho(Q)$.

Our main result is the following.

**Theorem 5.1.5.** Let $Q$ be a WCIP loop, let $\sigma$ be a permutation of $Q$ and let $c \in Q$.

1. If $\sigma$ is a right pseudoautomorphism of $Q$ with companion $c$, then $c \in N_\lambda(Q)$.

2. If $\sigma$ is a left pseudoautomorphism of $Q$ with companion $c$, then $c^{-1}$ is also a companion of $\sigma$ and $c^2 \in N_\lambda(Q)$.

**Proof.** (1) Since $1 = yy^{-1} = y \cdot x(x\backslash y^{-1})$, we have

$$c = 1\sigma \cdot c = y\sigma \cdot ((x(x\backslash y^{-1}))(\sigma \cdot c)) = y\sigma \cdot [x\sigma \cdot ((x\backslash y^{-1})\sigma \cdot c)].$$

Thus

$$x\sigma \backslash (y\sigma \backslash c) = (x\backslash y^{-1})\sigma \cdot c. \quad (5.1.1)$$
Exchanging the roles of x and y, we also have

\[ y\sigma \backslash (x\sigma \backslash c) = (y\backslash x^{-1})\sigma \cdot c. \] (5.1.2)

By (WCIP2), the right sides of 5.1.1 and 5.1.2 are equal, and so

\[ x\sigma \backslash (y\sigma \backslash c) = y\sigma \backslash (x\sigma \backslash c). \] (5.1.3)

Replacing x with \(x\sigma^{-1}\) and y with \(y\sigma^{-1}\) in 5.1.3, we have \(x\backslash (y\backslash c) = y\backslash (x\backslash c)\), and so

\[ x(y\backslash (x\backslash c)) = y\backslash c. \] (5.1.4)

Setting \(x = c\) in 5.1.4, we obtain

\[ y\backslash c = cy^{-1}. \] (5.1.5)

Using 5.1.5 in 5.1.4, we have

\[ x(y\backslash (cx^{-1})) = cy^{-1}. \] (5.1.6)

Taking \(y = cx^{-1}\) in 5.1.6, we get

\[ c(cx^{-1})^{-1} = x. \] (5.1.7)

Now in 5.1.6, replace \(x\) with \(cx^{-1}\) and use 5.1.7 and (WCIP2) to obtain

\[ cx^{-1} \cdot (x^{-1}\backslash y^{-1}) = cy^{-1}. \] (5.1.8)
Finally, in 5.1.8, replace \( x \) with \( x^{-1} \) and \( y \) with \( y^{-1} \), and then replace \( y \) with \( xy \) to get

\[
x \cdot y = c \cdot xy,
\]

which shows \( c \in N_\lambda(Q) \), as claimed.

(2) Since \((\sigma L_c, \sigma, \sigma L_c) \in \text{Atp}(Q)\), we have \((J \sigma L_c J, \sigma, J \sigma L_c J) \in \text{Atp}(Q)\) by Lemma 5.1.1. Since \(1\sigma = 1\), this autotopism lies in \(\text{Atp}_\lambda(Q)\). Thus \(J \sigma L_c J = \sigma L_d\) where \(d = 1J \sigma L_c J = c^{-1}\). Hence \((\sigma L_{c^{-1}}, \sigma, \sigma L_{c^{-1}}) \in \text{Atp}(Q)\), which shows that \(\sigma\) has \(c^{-1}\) as a companion. We have

\[
(L_{c^{-1}}^{-1} \sigma^{-1}, \sigma^{-1}, L_{c^{-1}}^{-1} \sigma^{-1}) (\sigma L_c, \sigma, \sigma L_c) = (L_{c^{-1}}^{-1} L_c, 1, L_{c^{-1}}^{-1} L_c) \in \text{Atp}(Q).
\]

Therefore \(L_{c^{-1}}^{-1} L_c = L_e\) where \(e = 1L_{c^{-1}}^{-1} L_c = c^2\). Thus \((L_{c^{-2}}, 1, L_{c^{-2}}) \in \text{Atp}(Q)\), that is, \(c^2 \in N_\lambda(Q)\). \(\square\)

**Corollary 5.1.6.** Let \(Q\) be a WCIP loop with trivial left nucleus. Then every right pseudoautomorphism is an automorphism. If, in addition, every element of \(Q\) has a unique square root, then every left pseudoautomorphism is an automorphism.

**Example 5.1.7.** The relativistic Bruck loop (or relativistic gyrocommutative gyrogroup) is the set of relativistic velocity vectors with Einstein’s velocity addition as the operation [47]. This is isomorphic to the natural Bruck loop structure on the set of positive definite symmetric Lorentz transformations [30, Ch. 10]. The left nucleus is trivial, because it is precisely the set of fixed points of the action of the special orthogonal group. In addition, every element of the loop has a unique square root. Thus we obtain: In the relativistic Bruck loop, every pseudoautomorphism is an automorphism.
Finally, we generalize a well-known result of Bruck [7], who proved the following for commutative Moufang loops.

**Corollary 5.1.8.** *Every pseudoautomorphism of a commutative, inverse property loop is an automorphism.*

*Proof.* In an inverse property loop, all nuclei coincide, so by Theorem 5.1.5 and its left/right dual, the companion of any pseudoautomorphism lies in the nucleus of $Q$. By Lemma 1.1.5, we have the desired result. 

\[\square\]
Bibliography


[23] T. Ikuta. Loops whose inner mappings are pseudo-automorphisms, I. Reports of Faculty of Science, 3:1–6, 1968.


Appendix A

GAP Functions

############################################################################
DeclareGlobalFunction( "GammaLoop", IsLoop );
############################################################################

##
##F GammaLoop( G )
##
## Returns the Gamma loop from a group (Bruck loop) of odd order.
##
#F GammaLoop( G )
##
## Returns the Gamma loop from a group (Bruck loop) of odd order.

InstallGlobalFunction( GammaLoop, function( G )

  local ej, ei, n, comm, squares, row, rowperm, i, j;
  n := Size( G );
  squares := List( [ 1..n ], i -> Elements(G)[i]*Elements(G)[i] );
  row := List([1..n], j-> []);
  rowperm := List([1..n], i-> []);
  for i in [1..n] do
    for j in [1..n] do
      ej := Elements(G)[j]; ei := Elements(G)[i];
      comm := ej^-1*ei^-1*ej*ei;
      row[j] := Position(Elements(G),ei*ej*Elements(G)[Position(squares,comm)]);
    od;
    rowperm[i] := PermList(row);
  od;
  return LoopByLeftSection(rowperm);

116
DeclareGlobalFunction( "BruckLoop", IsLoop );

#F BruckLoop( G )
#
## Returns the Bruck loop from a group (Gamma loop) of odd order.

InstallGlobalFunction( BruckLoop, function( G )

local n, ct, square, el_i, lsec, i, j;
n := Size( G );
ct := CanonicalCayleyTable( CayleyTable( G ) );
square := PermList(List( [ 1..n ], i -> ct[i][i] ));
lsec := [];
for i in [1..n] do
  el_i := Elements(G)[i];
  Add(lsec,
      square*RightTranslation(G,el_i)*
      LeftTranslation(G,RightDivision(el_i,el_i*el_i))^-1*square^-1
    );
  od;
return LoopByLeftSection( lsec );
end);

DeclareGlobalFunction( "LoopBJ", IsLoop );

#F LoopBJ( G )
##
## Returns the de Barros/Juriaans loop constructed from a loop <G>. This program is just a modification of the LoopMG2.

```
InstallGlobalFunction( LoopBJ, function( G )

local T, inv, n, L, i, j;

T := MultiplicationTable( Elements( G ) );
n := Size( G );
inv := List( [1..n], i->Position( T[i], 1 ) ); # inverses
L := List( [1..2*n], i->[] );

for i in [1..n] do for j in [1..n] do
L[i][j] := T[i][j]; # g*h = gh
L[i][j+n] := T[i][j] + n; # g*hu = (gh)u
L[i+n][j] := T[inv[j]][i] + n; # gu*h = (h^{-1}g)u
L[i+n][j+n] := T[i][inv[j]]; # gu*hu = gh^{-1}
od; od;

return LoopByCayleyTable( L );
end);
```

## GeneralLoopMG2 ( G , a)

```
InstallGlobalFunction( GeneralLoopMG2, function( G , a )

## GeneralLoopMG2 ( G , a)

## Returns the Chein MG2 loop constructed from a loop <G> and an center
## element a such that aa=1. This program is just a modification of the
## LoopMG2.

local T, inv, n, L, i, j;
T := MultiplicationTable( Elements( G ) );
a := Position(T[a],1);
```
\textbf{GeneralLoopBJ} \ \langle G \rangle \ \text{and} \ \langle \text{center element} \ a \rangle \\
\text{Returns the de Barros/Juriaans loop constructed from a loop } <G> \ \text{and} \ \text{an center element } a \ \text{such that } aa=1. \ \text{This program is just a modification} \ \text{of the LoopMG2}.
return LoopByCayleyTable( L );
end);

############################################################################
DeclareProperty( "IsSemiautomorphicIPLoop", IsLoop );

############################################################################
##
## IsSemiautomorphicIPLoop( Q )
##
## Determines if the left inner mapping group of Q is a subgroup
## of the automorphism group of Q.

InstallMethod( IsSemiautomorphicIPLoop, "for loop",
    [ IsLoop ],
    function( Q )
      return ( ForAll(Q,x-> ForAll(Q,y-> ForAll(Q,z->
        (x*y)*(z*(x*y))=x*(y*((z*x)*y))
      ))); end);

############################################################################
DeclareProperty( "IsARIFLoop", IsLoop );

############################################################################
##
## IsARIFLoop( Q )
##

InstallMethod( IsARIFLoop, "for loop",

[ IsLoop ],
function( Q )
return (
ForAll(Q,x-> ForAll(Q,y-> ForAll(Q,z->
  (z*x)*((y*x)*y)=(z*((x*y)*x))*y
 )));
); end);

############################################################################
InstallGlobalFunction( SomeSimpleRCCLoops, function( q )

##########################################################################
## SomeRCCLoops ( q )
##
## Returns a list of RCC loops constructed from GF( q )

local lps, g, cen, cc, rsec, mats, elm, img, a, b, i, j;
lps := [];
elm := Elements(GF(q));
g := GL(2,q);
cen := Center(g);
cc:=Filtered(ConjugacyClasses(g),x-> Size(x) = q*(q-1));
for i in [1..Size(cc)] do
  rsec := [];
mats := Union(cc[i],Elements(cen));
  for a in mats do
    b := List([1..q*q-1],i-> []);
    for j in [1..q*q-1] do
      img := [elm[QuoInt(j,q)+1],elm[RemInt(j,q)+1]]^a;
      b[j] := (Position(elm,img[1])-1)*q + Position(elm,img[2]) - 1;
    od;
    Add(rsec,PermList(b));
  od;
  Add(lps,LoopByRightSection(rsec));
od;

121
return(lps);
end);