A CLASS OF LOOPS CATEGORICALLY ISOMORPHIC TO UNIQUELY 2-DIVISIBLE BRUCK LOOPS

MARK GREER

ABSTRACT. We define a new variety of loops we call Γ-loops. After showing Γ-loops are power associative, our main goal will be showing a categorical isomorphism between uniquely 2-divisible Bruck loops and uniquely 2-divisible Γ-loops. 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). Finally, we answer a question posed by Jedlička, Kinyon and Vojtěchovský about the existence of Hall π-subloops and Sylow p-subloops in commutative automorphic loops. By showing commutative automorphic loops are Γ-loops and using the categorical isomorphism, we answer in the affirmative.

1. INTRODUCTION

A loop $(Q, \cdot)$ consists of a set Q with a binary operation $\cdot : Q \times Q \to Q$ such that (i) for all $a, b \in Q$, the equations $ax = b$ and $ya = b$ have unique solutions $x, y \in Q$, and (ii) there exists $1 \in Q$ such that $1x = x1 = x$ for all $x \in Q$. Standard references for loop theory are [2, 18].

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:

$$x \oplus y = (xy^2x)^{1/2}\,, \tag{1.1}$$

$$x \circ y = xy[y, x]^{1/2}\,. \tag{1.2}$$

Here $a^{1/2}$ denotes the unique $b \in Q$ satisfying $b^2 = a$ and $[y, x] = y^{-1}x^{-1}yx$. Then it turns out that both $(G, \oplus)$ and $(G, \circ)$ 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 $(G, \circ)$ all coincide.

For $(G, \oplus)$ all of this is well-known with the basic ideas dating back to Bruck [2] and Glauberman [6]. $(G, \oplus)$ is an example of a *Bruck loop*, that is, it satisfies the following identities

$$(x \oplus (y \oplus x)) \oplus z = x \oplus (y \oplus (x \oplus z)) \tag{Bol}$$

$$(x \oplus y)^{-1} = x^{-1} \oplus y^{-1} \tag{AIP}$$

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" [9].

2010 *Mathematics Subject Classification.* 20N05.

Key words and phrases. Γ-loops, Bruck loops, uniquely 2-divisible, power-associativity.

In the general case, $(G, \circ)$ turns out to live in a variety of loops which we will call Γ-*loops*. We defer the formal definition until §2, but note here that one defining axiom is commutativity. Γ-loops include as special cases two classes of loops which have appeared in the literature: commutative RIF loops [15] and commutative automorphic loops [11, 10, 12, 4]. We will not discuss RIF loops any further in this paper but we will review the notion of commutative automorphic loop in §2.

Jedlička, Kinyon and Vojtěchovský [11] showed that starting with a uniquely 2-divisible commutative automorphic loop $(Q, \circ)$, one can define a Bruck loop $(Q, \oplus')$ on the same underlying set Q by

$$x \oplus' y = (x^{-1} \backslash_\circ (y^2 \circ x))^{1/2} . \tag{1.3}$$

Here $a \backslash_\circ b$ is the unique solution c to $a \circ c = b$. We will extend this result to Γ-loops (Theorem 4.9). This gives us a functor $\mathcal{B} : \underline{\Gamma\mathrm{Lp}}_{1/2} \rightsquigarrow \underline{\mathrm{BrLp}}_{1/2}$ from the category $\underline{\Gamma\mathrm{Lp}}_{1/2}$ of uniquely 2-divisible Γ-loops to the category $\underline{\mathrm{BrLp}}_{1/2}$ of uniquely 2-divisible Bruck loops. One of our main results is the construction of an inverse functor $\mathcal{G} : \underline{\mathrm{BrLp}}_{1/2} \rightsquigarrow \underline{\Gamma\mathrm{Lp}}_{1/2}$, that is, $\mathcal{G} \circ \mathcal{B}$ is the identity functor on $\underline{\Gamma\mathrm{Lp}}_{1/2}$ and $\mathcal{B} \circ \mathcal{G}$ is the identity functor on $\underline{\mathrm{BrLp}}_{1/2}$.

Finite Bruck loops of odd order are known to have many remarkable properties, all established by Glauberman [6, 7]. For instance, they satisfy Lagrange's Theorem, the Odd Order Theorem, the Sylow and Hall Existence Theorems and finite Bruck p-loops (p odd) are centrally nilpotent. Using the isomorphism of the categories $\underline{\Gamma\mathrm{Lp}}_{1/2}$ and $\underline{\mathrm{BrLp}}_{1/2}$, we immediately get the same results for Γ-loops of odd order. We work out the details in §6. The Sylow and Hall Theorems for Γ-loops of odd order answer affirmatively an open problem of Jedlička, Kinyon and Vojtěchovský [11] in a more general way than was originally posed. Further, the proofs of the Odd Order Theorem and the nontriviality of the center of finite Γ-p-loops (p odd) are much simpler than the proofs in [11] and [12] for commutative automorphic loops.

We conclude this introduction with an outline of the rest of the paper. In §2 we give the complete definition of Γ-loop and we prove that for a uniquely 2-divisible group G, the construction (1.2) defines a Γ-loop on G. We also give examples of groups G such that $(G, \circ)$ is *not* automorphic. In §3, we prove that Γ-loops are power-associative (Theorem 3.5). As a consequence, for G a uniquely 2-divisible group, powers in G coincide with powers in $(G, \circ)$ (Corollary 3.6). In §4 we review the notion of twisted subgroup of a group and the connection between uniquely 2-divisible twisted subgroups and uniquely 2-divisible Bruck loops. In the special case where $(G, \circ)$ is a Γ-loop constructed on a uniquely 2-divisible group G, it turns out that $(G, \oplus) = (G, \oplus')$ (Theorem 4.13). As a consequence, if $(G, \circ)$ is the Γ-loop of a uniquely 2-divisible group G and if $(H, \circ)$ is a subloop of $(G, \circ)$, then H is a twisted subgroup of G (Corollary 4.14).

In §5 we construct the functor $\mathcal{G} : \underline{\mathrm{BrLp}}_{1/2} \rightsquigarrow \underline{\Gamma\mathrm{Lp}}_{1/2}$ and show that $\mathcal{B}$ and $\mathcal{G}$ are inverses of each other (Theorem 5.2). A loop is both a Bruck loop and a Γ-loop if and only if it is a commutative Moufang loop (Proposition 5.3) and we observe that restricted to such loops, both $\mathcal{B}$ and $\mathcal{G}$ are identity functors (Proposition 5.4).

In §6, we restrict the categorical isomorphism to finite loops of odd order, and derive the Odd Order, Sylow and Hall Theorems (Theorems 6.3, 6.7, and 6.8) for Γ-loops of odd order, as well as the nontriviality of the center of finite Γ-p-loops (p odd). Finally in §7, we conclude with some open problems.

2. Γ-loops

To avoid excessive parentheses, we use the following convention:

- multiplication $\cdot$ will be less binding than divisions $\backslash, /$.
- divisions are less binding than juxtaposition

For example $xy/z \cdot y\backslash xy$ reads as $((xy)/z)(y\backslash(xy))$. To avoid confusion when both $\cdot$ and $\circ$ are in a calculation, we denote divisions by $\backslash_\cdot$ and $\backslash_\circ$ respectively.

In a loop Q, the left and right translations by $x \in Q$ are defined by $yL_x = xy$ and $yR_x = yx$ respectively. We thus have $\backslash, /$ as $x\backslash y = yL_x^{-1}$ and $y/x = yR_x^{-1}$. We define *left multiplication group* of Q, $\mathrm{Mlt}_\lambda(Q) = \langle L_x \mid x \in Q\rangle$ and *multiplication group* of Q, $\mathrm{Mlt}(Q) = \langle R_x, L_x \mid x \in Q\rangle$. Similarly, we define the *inner mapping group* of Q, $\mathrm{Inn}(Q) = \mathrm{Mlt}_1(Q) = \{\theta \in \mathrm{Mlt}(Q) \mid 1\theta = 1\}$. A loop Q is an *automorphic loop* if every inner mapping of Q is an automorphism of Q, $\mathrm{Inn}(Q) \leq \mathrm{Aut}(Q)$.

In general, a loop Q is uniquely 2-divisible if the map $x \mapsto x^2$ is a bijection for all $x \in Q$. If Q is finite, we can say more about uniquely 2-divisible.

Theorem 2.1 ([11])**.** *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, Γ-loops, which we focus on in this paper.

Definition 2.2. *A loop $(Q, \cdot)$ is a Γ-loop if the following hold*

(Γ_1) Q *is commutative.*
(Γ_2) Q *has the automorphic inverse property (AIP):* $\forall x, y \in Q$, $(xy)^{-1} = x^{-1}y^{-1}$.
(Γ_3) $\forall x \in Q$, $L_x L_{x^{-1}} = L_{x^{-1}} L_x$.
(Γ_4) $\forall x, y \in Q$, $P_x P_y P_x = P_{yP_x}$ *where* $P_x = R_x L_{x^{-1}}^{-1} = L_x L_{x^{-1}}^{-1}$.

Note that a loop satisfying the AIP necessarily satisfies $(x\backslash y)^{-1} = x^{-1}\backslash y^{-1}$ and $(x/y)^{-1} = x^{-1}/y^{-1}$. We will use this without comment in what follows. The following identities are easily verified and will be used without reference.

Lemma 2.3. *Let G be a group. Then for all $x, y \in G$,*

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

Lemma 2.4. *Let G be a group. Then $xyx = \{x(y \circ x)x(y \circ x)^{-1}\}^{1/2}(y \circ x)$*

Proof. First note

$$\begin{aligned} yx(y\circ x)^{-1} &= yx(x^{-1}\circ y^{-1}) &&= yxx^{-1}y^{-1}[y^{-1},x^{-1}]^{1/2} \\ &= [y^{-1},x^{-1}]^{1/2} &&= (xyy^{-1}x^{-1}yxy^{-1}x^{-1})^{1/2} \\ &= (xy[y,x](xy)^{-1})^{1/2} &&= xy[y,x]^{1/2}(xy)^{-1} \\ &= (y\circ x)y^{-1}x^{-1} \end{aligned}$$

Hence we have

$$\{xyx(y\circ x)^{-1}\}^2 = x\,\underbrace{yx(y\circ x)^{-1}}\,xyx(y\circ x)^{-1} = x(y\circ x)y^{-1}x^{-1}xyx(y\circ x)^{-1}$$
$$= x(y\circ x)x(y\circ x)^{-1}\,.$$

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

Theorem 2.5. *Let G be a uniquely 2-divisible group. Then $(G,\circ)$ is a Γ-loop.*

Proof. For (Γ_1) we have

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

Similarly for (Γ_2),

$$\begin{aligned} x^{-1}\circ y^{-1} &= x^{-1}y^{-1}[y^{-1},x^{-1}]^{1/2} \quad = (yx)^{-1}([y,x]^{(yx)^{-1}})^{1/2} \\ &= (yx)^{-1}([y,x]^{1/2})^{(yx)^{-1}} = [y,x]^{1/2}(yx)^{-1} = (yx[x,y]^{1/2})^{-1} \\ &= (y\circ x)^{-1}\,. \end{aligned}$$

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

$$\begin{aligned} x &= \{a^{-1}ba^{-1}b^{-1}\}^{1/2}b && \Leftrightarrow \\ (xb^{-1})^2 &= a^{-1}ba^{-1}b^{-1} && \Leftrightarrow \\ xb^{-1}x &= aba^{-1} && \Leftrightarrow \\ xa &= bx^{-1}a^{-1}b && \Leftrightarrow \\ [x,a] &= (x^{-1}a^{-1}b)^2 && \Leftrightarrow \\ ax[x,a]^{1/2} &= b && \Leftrightarrow \\ xL_a &= b. \end{aligned}$$

For (Γ_3), first note

$$x^{-1}\circ xy = y[xy,x^{-1}]^{1/2} = y[x,yx^{-1}]^{1/2} = yx^{-1}\circ x. \tag{2.1}$$

Similarly,

$$x^{-1}\circ y = x^{-1}y[y,x^{-1}]^{1/2} = x^{-1}y([x,y]^{1/2})^{x^{-1}} = y[y,x][x,y]^{1/2}x^{-1} = y[x,y]^{1/2}x^{-1}. \tag{2.2}$$

Therefore

$$x^{-1}\circ(x\circ y) = x^{-1}\circ(xy[y,x]^{1/2}) \overset{(2.1)}{=} x\circ(y[y,x]^{1/2})x^{-1} \overset{(2.2)}{=} x\circ(x^{-1}\circ y).$$

For (Γ_4), rewriting Lemma 2.4 gives $xyx=\{x(y\circ x)x(y\circ x)^{-1}\}^{1/2}(y\circ x) = x^{-1}\backslash_\circ(y\circ x)$. Let $y\Psi_x = xyx$, and observe $P_xP_yP_x = \Psi_x\Psi_y\Psi_x = \Psi_{y\Psi_x} = P_{yP_x}$. □

Remark 2.6. Let G be a uniquely 2-divisible group. The proof of Theorem 2.5 gives the following expression for $\backslash_\circ$:

$$a\backslash_\circ b = \{a^{-1}ba^{-1}b^{-1}\}^{1/2}b\,.$$

Using this in Lemma 2.4 gives $xyx = x^{-1}\backslash_\circ(y\circ x) = yP_x$.

Lemma 2.7. *Commutative automorphic loops are Γ-loops.*

Proof. This follows from Lemmas 2.6, 2.7 and 3.3 in [11]. □

Example 2.8. *The smallest example known of an odd order* Γ*-loop that is not automorphic has order* 375*, which corresponds to the smallest group of odd order that is not metabelian. Its GAP library number is* $[375, 2]$.

Example 2.9. *The following is the smallest* Γ*-loop which is neither a commutative automorphic nor commutative RIF loop, found by* Mace4 [16].

$\cdot$	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

3. Γ-Loops are power-associative

In a Γ-loop Q, define $x^n = 1L_x^n$ for all $n \in \mathbb{Z}$.

Proposition 3.1. *Let* Q *be a* Γ*-loop. Then* $x^{-n} = (x^{-1})^n = (x^n)^{-1}$.

Proof. The first equality, $(1)L_x^{-n} = (1)L_{x^{-1}}^n$, is equivalent to $1 = (1)L_{x^{-1}}^n L_x^n$. By (Γ_3), $L_{x^{-1}}^n L_x^n = (L_{x^{-1}} L_x)^n$. But since $L_{x^{-1}} L_x \in \mathrm{Inn}(Q)$, we are done. The second equality follows from (Γ_2). □

Proposition 3.2. *Let* Q *be a* Γ*-loop. Then*

$$(P_1) \qquad P_x = L_x L_{x^{-1}}^{-1} = L_{x^{-1}}^{-1} L_x$$

$$(P_2) \qquad P_x L_x = L_x P_x$$

Proof. These follow from (Γ_3). □

Lemma 3.3. *Let* Q *be a* Γ*-loop. Then* $\forall k, n \in \mathbb{Z}$ *we have the following:*

(a) $x^n P_x = x^{n+2}$
(b) $P_x^n = P_{x^n}$
(c) $x^k P_{x^n} = x^{k+2n}$

Proof. For (a), if $n = 0$, we need $x^{-1} \backslash x = x^2$, that is, $x^{-1} x^2 = x$. But this follows from (Γ_3). For general n, we have

$$x^n P_x = 1L_x^n P_x \overset{(P_2)}{=} 1P_x L_x^n = x^2 L_{x^n} = 1L_x^2 L_x^n = 1L_x^{n+2} = x^{n+2}\,.$$

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

$$P_x^n = P_x P_x^{n-2} P_x = P_x P_{x^{n-2}} P_x \overset{(\Gamma_4)}{=} P_{x^{n-2} P_x} \overset{(a)}{=} P_{x^n}\,.$$

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

$$P_x^{-n} = (P_x^n)^{-1} = P_{x^n}^{-1} = P_{(x^n)^{-1}} = P_{x^{-n}}\,,$$

by Proposition 3.1.

For (c), let k be fixed. Then

$$x^k P_{x^n} \overset{(b)}{=} x^k P_x^n \overset{(a)}{=} x^{k+2} P_x^{n-1} \overset{(a)}{=} \dots \overset{(a)}{=} x^{k+2n}\,. \qquad \square$$

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

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

Lemma 3.4. *Let Q be a Γ-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) $i \in \{-m-1, \dots, m+1\}$, $j \in \{-m, \dots, m\}$,
(2) $i \in \{-m, \dots, m\}$, $j = m+1$ or $j = -m-1$,
(3) $i = m+1$, $j = -m-1$ or $i = -m-1$, $j = m+1$,
(4) $i = m+1$, $j = m+1$ or $i = -m-1$, $j = -m-1$,
(5) $i \in \{-m-1, \dots, m+1\}$, $j = m+2$ or $j = -m-2$.

By (Γ_2) and Proposition 3.1, $x^i x^j = x^{i+j}$ 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 PA(m) (with the roles of i and j reversed) and commutativity. Case (2) also follows from PA(m). Case (3) follows from Proposition 3.1: $x^{m+1} x^{-m-1} = x^{m+1} x^{-(m+1)} = 1$.

For case (4),

$$x^{m+1} x^{m+1} = (1) L^{-1}_{x^{-(m+1)}} L_{x^{m+1}} \overset{(P_1)}{=} (1) P_{x^{m+1}} \overset{(3.3c)}{=} x^{2m+2}\,.$$

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

$$x^i x^{m+2} = (x^{m+2}) P_{x^i} L_{x^{-i}} \overset{(3.3c)}{=} x^{-i} x^{m+2+2i} \overset{\mathrm{PA}(m)}{=} x^{m+2+i}\,.$$

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

$$x^i x^{m+2} \overset{(3.3c)}{=} (x^{m+2-2i}) P_{x^i} L_{x^i} \overset{(P_2)}{=} (x^i x^{m+2-2i}) P_{x^i} \overset{\mathrm{PA}(m)}{=} (x^{m+2-i}) P_{x^i} \overset{(3.3c)}{=} x^{m+2+i}\,. \qquad \square$$

Theorem 3.5. *Γ-loops are power associative.*

Proof. This follows immediately from Lemma 3.4. Indeed, $x^k x^\ell = x^{k+\ell}$ with $0 \leq |k| \leq |\ell|$ follows from PA($|\ell|$). $\square$

By Theorem 2.5 and Theorem 3.5, for a uniquely 2-divisible group G and its corresponding Γ-loop $(G, \circ)$, we have powers coinciding.

Corollary 3.6. *Let G be a uniquely 2-divisible group and $(G, \circ)$ its associated Γ-loop. Then powers in G coincide with powers in $(G, \circ)$.*

4. Twisted subgroups and uniquely 2-divisible Bruck loops

We turn to an idea from group theory, first studied by Aschbacher [1]. We follow the notations and definitions used by Foguel, Kinyon and Phillips [5], and refer the reader to that paper for a more complete discussion of the following results.

Definition 4.1. *A* twisted subgroup *of a group G is a subset $T \subset G$ such that $1 \in T$ and for all $x, y \in T$, $x^{-1} \in T$ and $xyx \in T$.*

Example 4.2 ([5])**.** *Let G be a group and $\tau \in \mathrm{Aut}(G)$ with $\tau^2 = 1$. Let $K(\tau) = \{g \in Q \mid g\tau = g^{-1}\}$. Then $K(\tau)$ is a twisted subgroup.*

Lemma 4.3. *Let G be uniquely 2-divisible group and let $\tau \in \mathrm{Aut}(G)$ satisfy $\tau^2 = 1$. Then $K(\tau)$ is closed under $\circ$ and $\backslash_\circ$ 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 (Γ_2). Similarly, (Γ_2) also gives $(x\backslash_\circ y)\tau = (x\backslash_\circ y)^{-1}$. □

Theorem 4.4 ([5])**.** *Let Q be a Bruck loop. Then L_Q is a twisted subgroup of $\mathrm{Mlt}_\lambda(Q)$. If Q has odd order, then $\mathrm{Mlt}_\lambda(Q)$ has odd order. Moreover, there exists a unique $\tau \in \mathrm{Aut}(\mathrm{Mlt}_\lambda(Q))$ where $\tau^2 = 1$ and $L_Q = \{\theta \in \mathrm{Mlt}_\lambda(Q) \mid \theta\tau = \theta^{-1}\}$. On generators, $(L_x)^\tau = L_{x^{-1}}$.*

Corollary 4.5. *Let $(Q, \cdot)$ be a uniquely 2-divisible Bruck loop. Then $(L_Q, \circ)$ is a Γ-loop.*

Proof. This follows from Lemma 4.3 and Theorem 4.4 □

We have a bijection from Q to L_Q given by $x \mapsto 1L_x$. This allows us to define a Γ-loop operation directly on Q as follows:

$$x \circ y = 1(L_x \circ L_y)$$

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

Proposition 4.6. *Let $(Q, \cdot)$ be a uniquely 2-divisible Bruck loop. Then $(Q, \circ)$ is a Γ-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 [19], $x^n = 1L_{x^n} = 1L_x^n$. By Corollary 3.6, L_x^n coincides with the nth power of L_x in $(L_Q, \circ)$. Thus x^n is the nth power of x in $(Q, \circ)$. Since this argument is clearly reversible, we have the desired result. □

Recalling the definitions of $\oplus$ and $\oplus'$ as

$$x \oplus y = (x^{-1}\backslash.(y^2 x))^{1/2}$$
$$x \oplus' y = (x^{-1}\backslash_\circ(y^2 \circ x))^{1/2}$$

for Γ-loops $(Q, \cdot)$ and $(Q, \circ)$, we now generalize Lemma 3.5 of Jedlička, Kinyon and Vojtěchovský [11].

Remark 4.7. In what follows, we will always denote our starting structure as $(Q,\cdot)$. $(Q,\circ)$ will always denote the associated Γ-loop and $(Q,\oplus)$, $(Q,\oplus')$ will denote the associated Bruck loops of $(Q,\cdot)$ and $(Q,\circ)$, respectively.

Proposition 4.8. *Let Q be a Γ-loop. Then*

$$(yP_x)^2 = x^2 P_y P_x.$$

Proof. By Proposition 3.3(a), we have that $x^2 = 1P_x$. Hence, $x^2 P_y P_x = 1P_x P_y P_x \overset{(\Gamma_4)}{=} 1P_{yP_x} = (yP_x)^2$ by Proposition 3.3(a) again. □

Theorem 4.9. *Let $(Q,\cdot)$ be a uniquely 2-divisible Γ-loop. Then $(Q,\oplus)$ is a Bruck loop. Moreover, powers in $(Q,\cdot)$ coincide with powers in $(Q,\oplus)$.*

Proof. Let $x\delta = x^2$ and note that $yL_x = x\oplus y = (x^{-1}\backslash(y^2x))^{1/2} = y\delta P_x\delta^{-1}$. Thus,

$$L_xL_yL_x = \delta P_x\delta^{-1}\delta P_y\delta^{-1}\delta P_x\delta^{-1} = \delta P_xP_yP_x\delta^{-1} \overset{(\Gamma_4)}{=} \delta P_{yP_x}\delta^{-1}.$$

But by Proposition 4.8,

$$yP_x = (x^2P_yP_x)^{1/2} = (x^{-1}\backslash[(y^{-1}\backslash(x^2y))x])^{1/2} = x\oplus(y^{-1}\backslash(x^2y))^{1/2} = x\oplus(y\oplus x).$$

Thus,

$$L_xL_yL_x = \delta P_{yP_x}\delta^{-1} = \delta P_{x\oplus(y\oplus x)}\delta^{-1} = L_{x\oplus(y\oplus x)}.$$

The fact that $(Q,\oplus)$ has AIP is straightforward from (Γ_2). Powers coinciding follows from power associativity. □

Given a uniquely 2-divisible Bruck loop $(Q,\cdot)$ wish the give the explicit equation of the left division operation in $(Q,\circ)$. We will need the following two facts for Bol loops, both well known.

Proposition 4.10 ([6, 19])**.** *Let Q be a Bol loop. Then the following are equivalent:*

(i) $(xy)^{-1} = x^{-1}y^{-1}$, *and*
(ii) $(xy)^2 = x\cdot y^2x$.

Proposition 4.11 ([14])**.** *Let Q be a Bol loop. Then $x/y = y^{-1}(yx\cdot y^{-1})$.*

Proposition 4.12. *Let $(Q,\cdot)$ be a uniquely 2-divisible Bruck loop and let $(Q,\circ)$ be its Γ-loop. For all $a,b\in Q$,*

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

Proof. Let $a,b\in(Q,\circ)$ b fixed and set $x = (a^{-1}b^{1/2})/.b^{-1/2}$. Then $xb^{-1/2} = a^{-1}b^{1/2}$ by Proposition 4.11. This give $x\cdot b^{-1}x = a^{-1}\cdot ba^{-1}$ by Proposition 4.10(ii). 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 $L_xL_b^{-1}L_x = L_a^{-1}L_bL_a^{-1}$. This in turn is equivalent to $[L_a,L_x] = (L_a^{-1}L_x^{-1}L_b)^2$ and therefore $L_xL_a[L_a,L_x]^{1/2} = L_b$. Hence, $1(L_x\circ L_a) = 1L_b \Rightarrow x\circ a = b$. □

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

Theorem 4.13. *Let $(G,\cdot)$ be a uniquely 2-divisible group. Then $(G,\oplus) = (G,\oplus')$.*

Proof. By Remark 2.6, we have $xyx = yP_x$ for all $x, y \in G$. Replacing y by y^2 and applying square roots gives $x \oplus y = (xy^2x)^{1/2} = (y^2P_x)^{1/2} = (x^{-1}\backslash_\circ(y^2 \circ x))^{1/2} = x \oplus' y$. □

Corollary 4.14. *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 we have $xyx = yP_x \in H$ for all $x, y \in H$. □

5. Inverse functors

We will need the following lemma for our main result.

Lemma 5.1. *Let $(Q, \cdot)$ be a uniquely 2-divisible Γ-loop and $(Q, \oplus)$ be its Bruck loop. Then*

$$x \oplus (xy)^{-1/2} = y^{-1} \oplus (xy)^{1/2}\,. \tag{5.1}$$

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

$$\begin{aligned} x^{-1}\backslash(x^{-1}y^{-1} \cdot x) &\overset{(\Gamma_1)}{=} x^{-1}\backslash(x \cdot x^{-1}y^{-1}) \overset{(\Gamma_3)}{=} x^{-1}\backslash(x^{-1} \cdot xy^{-1}) = xy^{-1} \\ &\overset{(\Gamma_1)}{=} y^{-1}x = y\backslash(y \cdot y^{-1}x) \overset{(\Gamma_3)}{=} y\backslash(y^{-1} \cdot yx) \overset{(\Gamma_1)}{=} y\backslash(yx \cdot y^{-1})\,. \end{aligned}$$ □

Now let $\mathcal{G} : \underline{\mathrm{BrLp}}_{1/2} \rightsquigarrow \underline{\Gamma\mathrm{Lp}}_{1/2}$ be the functor given on objects by assigning to each uniquely 2-divisible Bruck loop $(Q, \cdot)$ its corresponding Γ-loop $(Q, \circ)$, and let $\mathcal{B} : \underline{\Gamma\mathrm{Lp}}_{1/2} \rightsquigarrow \underline{\mathrm{BrLp}}_{1/2}$ be the functor given on objects by assigning to each uniquely 2-divisible Γ-loop $(Q, \cdot)$ its corresponding Bruck loop $(Q, \oplus)$.

Theorem 5.2.

(A) *$\mathcal{G} \circ \mathcal{B}$ is the identity functor on $\underline{\Gamma\mathrm{Lp}}_{1/2}$.*

(B) *$\mathcal{B} \circ \mathcal{G}$ is the identity functor on $\underline{\mathrm{BrLp}}_{1/2}$.*

Proof. (A) Let $(Q, \cdot)$ be a uniquely 2-divisible Γ-loop, let $(Q, \oplus)$ be its corresponding Bruck loop and let $(Q, \circ)$ be the Γ-loop of $(Q, \oplus)$. Lemma 5.1 and Proposition 4.12 imply $x = (y^{-1} \oplus (xy)^{1/2})/_\oplus(xy)^{-1/2} = (xy)/_\circ y$. Thus $xy = x \circ y$, as claimed.

(B) Let $(Q, \cdot)$ be a uniquely 2-divisible Bruck loop, let $(Q, \circ)$ be its corresponding Γ-loop and let $(Q, \oplus')$ be the Bruck loop of $(Q, \oplus)$. 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

$$\begin{aligned} L_{(x\oplus' y)^2} &= L_{x^{-1}\backslash_\circ(y^2\circ x)} = L_x^{-1}\backslash_\circ(L_y^2 \circ L_x) = (L_x \oplus' L_y)^2 \\ &= (L_x \oplus L_y)^2 = L_x L_y^2 L_x \qquad = L_{x\cdot(y^2\cdot x)} \\ &= L_{(xy)^2}\,, \end{aligned}$$

using Theorem 4.13 and Proposition 4.10(ii). Thus $(xy)^2 = (x \oplus' y)^2$ and so the desired result follows from taking square roots. □

We note in passing that we have proven a result which can be stated purely in terms of uniquely 2-divisible Bruck loops:
Let $(Q, \cdot)$ be a uniquely 2-divisible Bruck loop. For each $x, y \in Q$, the equation

$$xz^{-1/2} = y^{-1}z^{1/2} \tag{$\star$}$$

has a unique solution $z \in Q$.

We conclude this section by discussing the intersection of the varieties of Bruck loops and Γ-loops.

Proposition 5.3. *A loop is both a Bruck loop and* Γ*-loop if and only if it is a commutative Moufang loop.*

Proof. Commutative Bol loops are commutative Moufang loops [20]. □

Proposition 5.4. *Let* $(Q, \cdot)$ *be a uniquely* 2*-divisible commutative Moufang loop. Then* $(Q, \cdot) = (Q, \circ) = (Q, \oplus)$*.*

Proposition 5.5. *Let* $(Q, \cdot)$ *be a* Γ*-loop of exponent* 3*. Then* $(Q, \cdot)$ *is a commutative Moufang loop.*

Proof. The Bruck loop $(Q, \oplus)$ is a commutative Moufang loop [20]. Since its Γ-loop coincides with $(Q, \cdot)$ by Theorem 5.2, the desired result follows from Proposition 5.4. □

6. Γ-loops of odd order

We restrict the categorical isomorphism to finite loops of odd order and reap the benefits of the known structure for Bruck loops by Glauberman [6, 7]. By the categorical isomorphism, Theorem 5.2, if $(Q, \cdot)$ is a Bruck loop, then $(Q, \cdot) = (Q, \oplus)$. We will use this without reference in what follows.

Proposition 6.1. *Let* $(Q, \cdot)$ *be a* Γ*-loop with* $|Q| = p^2$ *for* p *prime. Then* $(Q, \cdot)$ *is an abelian group.*

Proof. Loops of order 4 are abelian groups [18]. For odd primes, Bol loops of order p^2 are abelian groups [3]. Hence, by Theorem 5.2, the Γ-loop of $(Q, \oplus)$ coincides with $(Q, \cdot)$. □

Lemma 6.2. *Let* $(Q, \cdot)$ *be a uniquely* 2*-divisible* Γ*-loop 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 5.2), any normal subloop of $(Q, \oplus)$ is a normal subloop of $(Q, \cdot)$ and vice versa. 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. □

Theorem 6.3 (Odd Order Theorem)**.** Γ*-loops of odd order are solvable*

Proof. Let $(Q, \cdot)$ be a Γ-loop of odd order and let $(Q, \oplus)$ be its Bruck loop. Then $(Q, \oplus)$ is solvable ([7], Theorem 14(b), p. 412), and so the desired result follows from Lemma 6.2. □

Theorem 6.4 (Lagrange and Cauchy Theorems)**.** *Let* $(Q, \cdot)$ *be a finite* Γ*-loop of odd order. Then:*

(L) *If* $A \leq B \leq Q$ *then* $|A|$ *divides* $|B|$.
(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 ([6], Corollary 4, p. 395). Similarly, if an odd prime p divides $|Q|$, then $(Q, \oplus)$ has an element of order p ([6], Corollary 1, p. 394). Hence, Q has an element of order p. □

Theorem 6.5. *Let* Q *be a finite* Γ*-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 6.6. Note that this is false for $p = 2$ by Example 2.9.

Proof. If $|Q|$ is a power of p, then by Theorem 6.4(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 6.4(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 Γ-loops. Moreover, we can now show the existence of Hall π-subloops and Sylow p-subloops.

Theorem 6.7 (Sylow subloops)**.** Γ*-loops of odd order have Sylow* p*-subloops.*

Proof. Let $(Q, \cdot)$ be a Γ-loop of odd order and $(Q, \oplus)$ its Bruck loop. Then $(Q, \oplus)$ has a Sylow p-subloop ([6], Corollary 3, p. 394), say $(P, \oplus)$. But then $(P, \circ)$ is a Sylow p-subloop of $(Q, \cdot)$ by Theorem 5.2. □

Theorem 6.8 (Hall subloops)**.** Γ*-loops of odd order have Hall* π*-subloops.*

Proof. Let $(Q, \cdot)$ be a Γ-loop of odd order and $(Q, \oplus)$ its Bruck loop. Then $(Q, \oplus)$ has a Hall π- subloop ([6], Theorem 8, p. 392), say $(H, \oplus)$. But then $(H, \circ)$ is a Hall π-subloop of $(Q, \cdot)$ by Theorem 5.2. □

Recall the *center* of a loop Q is defined as

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

Theorem 6.9. *Let* $(Q, \cdot)$ *be a uniquely* 2*-divisible Bruck loop. 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 5.1 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 $x, y, z \in Q$,

$$z[L_y, L_{xa}] = zL_y^{-1} L_{xa}^{-1} L_y L_{xa} = xa \cdot y((xa)^{-1} \cdot y^{-1} z) = x \cdot y(x^{-1} \cdot y^{-1} z) = z[L_y, L_x].$$

Thus, for all $x, y \in Q$,

$$\begin{aligned} (a \circ x) \circ y = ax \circ y \quad &= L_{ax} \circ L_y &&= L_a L_x \circ L_y \\ = L_a L_x L_y [L_y, L_a L_x]^{1/2} &= L_a L_x L_y [L_y, L_x]^{1/2} &&= L_a L_{x \circ y} \\ = L_{a(x \circ y)} \quad &= L_{a \circ (x \circ y)} &&= a \circ (x \circ y)\,. \end{aligned}$$

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. Then we have

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

Moreover,

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

Therefore $a\in Z(Q,\cdot)$ since $(Q,\cdot)$ is a Bruck loop. □

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 6.10. *Let p be an odd prime. Then uniquely 2-divisible Γ 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 ([6], Theorem 7, p. 390). Therefore, $(Q,\cdot)$ is centrally nilpotent of class n. □

7. Conclusion

It is appropriate to think of uniquely 2-divisible Γ-loops, besides forming a category, as forming a variety with the square root function $^{1/2}$ as part of the signature. The same applies to uniquely 2-divisible Bruck loops.

The multiplication in the Bruck loop of a Γ-loop is explicitly given as a term operation in the language of Γ-loops by $x\oplus y=(x^{-1}\backslash(y^2x))^{1/2}$. However, we were not able to do the same for the multiplication in the Γ-loop of a Bruck loop. In the latter variety, ($\star$) gives a uniquely determined z for each x,y.

Problem 7.1. *Let $(Q,\cdot)$ be a Bruck loop. Does there exist a term for $x\circ y$ in the language of Bruck loops?*

Problem 7.2. *Let $(Q,\cdot)$ be a Bruck loop of order p^3 where p is an odd prime. Is $(Q,\circ)$ is a commutative automorphic loop?*

If this holds, then a classification of Bruck loops of order p^3 would follow from [4] and Theorem 5.2.

Acknowledgment. I would like to thank Michael Kinyon for suggesting this problem and for his careful reading of each draft of the manuscript. Some investigations in this paper were assisted by the automated deduction tool Prover9 [16], the finite model builder Mace4 [16] and GAP with the LOOPS package [8, 17].

References

1. M. Aschbacher, *Near subgroups of finite groups*, J. Group Theory **1** (1998), 113–129.
2. R. H. Bruck, *A Survey of Binary Systems*, Springer-Verlag, Berlin, 1971.
3. R.P. Burn, *Finite bol loops*, Math. Proc. Cambridge Philos. Soc. **84** (1978), 377–385.
4. D. A. S. de Barros, A. Grishkov, and P. Vojtěchovský, *Commutative automorphic loops of order p^3*, Journal of Algebra and its Applications (to appear).
5. T. Foguel, M. K. Kinyon, and J. D. Phillips, *On twisted subgroups and bol loops of odd order*, Rocky Mountain J. Math **36** (2006), 183–212.

6. G. Glauberman, *On loops of Odd Order I*, Journal of Algebra **1** (1964), 374–396.
7. ———, *On loops of Odd Order II*, Journal of Algebra **8** (1968), 393–414.
8. The GAP Group, *Groups, Algorithms, and Programming*, http://www.gap-system.org (2008).
9. I.M. Isaacs, *Finite group theory*, Graduate studies in mathematics **92** (2008).
10. P. Jedlička, M.K. Kinyon, and P. Vojtěchovský, *Constructions of commutative automorphic loops*, Comm. Algebra **38** (2010), 3243–3267.
11. ———, *The structure of commutative automorphic loops*, Trans. Amer. Math. Soc. **363** (2011), 365–384.
12. ———, *Nilpotency in automorphic loops of prime power order*, Journal of Algebra **350** (2012), 64–76.
13. K. W. Johnson, M.K. Kinyon, G. P. Nagy, and P. Vojtěchovský, *Searching for small simple automorphic loops*, LMS Journal of Computation and Mathematics **14** (2011), 200–213.
14. Hubert Kiechle, *Theory of K-Loops*, vol. 1778, Lecture Notes in Mathematics, 2002.
15. M. K. Kinyon and Petr Vojtěchovský, *Primary Decompositions in Varieties of commutative diassociative loops*, Communications in Algebra **37** (2009), 1428–1444.
16. W. McCune, *Prover9 and Mace4*, http://www.cs.unm.edu/˜mccune/prover9/ (2009).
17. G. P. Nagy and P. Vojtěchovský, *Loops: Computing with quasigroups and loops*, http://www.math.du.edu/loops (2008).
18. H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math, Berlin, 1990.
19. D.A. Robinson, *Bol loops*, Trans. Amer. Math. Soc. **123** (1966), 341–354.
20. ———, *Bol quasigroups*, Publ. Math. Debrecen **19** (1972), 151–153.

E-mail address: `mark.greer@du.edu`

Department of Mathematics, 2360 S Gaylord St., University of Denver, Denver, CO 80208 USA