TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 363, Number 1, January 2011, Pages 365–384
S 0002-9947(2010)05088-3
Article electronically published on August 16, 2010

THE STRUCTURE OF COMMUTATIVE AUTOMORPHIC LOOPS

PŘEMYSL JEDLIČKA, MICHAEL KINYON, AND PETR VOJTĚCHOVSKÝ

Abstract. An *automorphic loop* (or *A-loop*) is a loop whose inner mappings are automorphisms. Every element of a commutative A-loop generates a group, and $(xy)^{-1} = x^{-1}y^{-1}$ holds. Let Q be a finite commutative A-loop and p a prime. The loop Q has order a power of p if and only if every element of Q has order a power of p. The loop Q decomposes as a direct product of a loop of odd order and a loop of order a power of 2. If Q is of odd order, it is solvable. If A is a subloop of Q, then $|A|$ divides $|Q|$. If p divides $|Q|$, then Q contains an element of order p. If there is a finite simple nonassociative commutative A-loop, it is of exponent 2.

1. Introduction

A *loop* $(Q, \cdot)$ is a set Q with a binary operation $\cdot$ such that (i) for each $x \in Q$, the *left translation* $L_x : Q \to Q; y \mapsto yL_x = xy$ and the *right translation* $R_x : Q \to Q; y \mapsto yR_x = yx$ are bijections, and (ii) there exists $1 \in Q$ satisfying $1 \cdot x = x \cdot 1 = x$ for all $x \in Q$. The left and right translations generate the *multiplication group* $\mathrm{Mlt}(Q) = \langle L_x, R_x \mid x \in Q \rangle$. The *inner mapping group* $\mathrm{Inn}(Q) = \mathrm{Mlt}(Q)_1$ is the stabilizer of $1 \in Q$. Standard references for the theory of loops are [4, 5, 17].

A loop Q is an *automorphic loop* (or *A-loop*) if every inner mapping of Q is an automorphism of Q, that is, $\mathrm{Inn}(Q) \leq \mathrm{Aut}(Q)$. Thus the class of A-loops, which is certainly not the class of all loops, includes, for instance, groups and commutative Moufang loops [5].

The study of A-loops was initiated by Bruck and Paige [6]. They obtained many basic structural results for A-loops and also described some constructions. The bulk of [6] was devoted to the (implicitly stated) problem of whether every *diassociative* A-loop, that is, an A-loop in which every 2-generated subloop is a group, is a Moufang loop. Affirmative answers were given by Osborn [16] in the commutative case, and Kinyon, Kunen and Phillips [13] in the general case. Moufang A-loops have been used to characterize a certain class of quasigroups [12] and have been shown to have an affirmative answer for the restricted Burnside problem [18].

By contrast, the study of other classes of A-loops has lain quite fallow. In this paper, we give a detailed structure theory for *commutative* A-loops. Here is a summary of our main results:

In §2, we present preliminary results which will be used throughout the rest of the paper. Some of these results, such as the power-associativity of commutative

Received by the editors October 6, 2008 and, in revised form, March 31, 2009.
2010 *Mathematics Subject Classification.* Primary 20N05.
The first author was supported by the Grant Agency of the Czech Republic, grant no. 201/07/P015.

A-loops (Lemma 2.4), are already known for arbitrary A-loops [6], but we give short proofs to make the present paper self-contained. Other results, such as the automorphic inverse property (Lemma 2.6) are new.

In §3, we study commutative A-loops of odd order, i.e. finite A-loops in which every element has odd order (Lemma 3.1). The multiplication group of a commutative A-loop contains a natural (but not at all obvious) twisted subgroup (Lemma 3.3). In the odd order case, this enables us to construct a new loop operation on a commutative A-loop with the property that powers in the new loop coincide with powers in the original loop (Lemma 3.5). The new loop is in fact a *Bruck loop*, and we exploit this fact to establish *Lagrange* and *Cauchy* Theorems for commutative A-loops of odd order (Propositions 3.6 and 3.7). Our main result in §3 is the *Odd Order Theorem*: every commutative A-loop of odd order is solvable (Theorem 3.12).

In §4, we turn to a property trivially satisfied in abelian groups and valid in commutative Moufang loops thanks to dissociativity: the product of squares is a square. This turns out be true in commutative A-loops as well (Theorem 4.1), despite the fact that the naive formula $x^2y^2 = (xy)^2$ does not hold in general. Instead, $x^2y^2 = (x \diamond y)^2$ for a rather complicated binary operation $\diamond$; in the Moufang case, $\diamond$ coincides with the original operation. Following the same philosophy as in the odd order case, we study the new operation $\diamond$ and note that it defines a commutative, power-associative loop on the same underlying set as the original commutative A-loop. In the odd order case, $\diamond$ yields an isomorphic copy of the original loop (Lemma 4.6), but at the other extreme where every element has order a power of 2, the new loop operation $\diamond$ turns out to have strong structural properties, as we will show in later sections.

In §5, we prove a *Decomposition Theorem*: every finite commutative A-loop is a direct product of a subloop of odd order and a subloop in which every element has order a power of 2 (Theorem 5.1). This is a generalization of the familiar decomposition theorems in abelian groups and commutative Moufang loops. Unlike those cases, however, no further decomposition is possible: commutative A-loops of odd order are not necessarily direct products of p-loops for odd p.

In §6, we examine commutative A-loops of exponent 2. This special case is of particular importance because of a straightforward consequence of the Decomposition Theorem and the Odd Order Theorem, namely that a finite, simple, commutative A-loop is either a cyclic group of odd prime order or it has exponent 2 (Proposition 6.1). To study the exponent 2 case, we return to the new loop operation $\diamond$ introduced in §4, and prove the main result of §6: if Q is a finite, commutative A-loop of exponent 2, then $(Q, \diamond)$ is an elementary abelian 2-group (Theorem 6.2). An immediate corollary of this is that a commutative A-loop of exponent 2 has order a power of 2 (Corollary 6.3).

In §7, we briefly examine p-loops. The main result is that the two reasonable definitions of this notion coincide for commutative A-loops, that is, a finite commutative A-loop has order a power of p if and only if every element has order a power of p (Theorem 7.1). For p odd, this is a consequence of the Lagrange and Cauchy Theorems. For $p = 2$, it follows from the Decomposition Theorem and the fact that it has already been observed in the exponent 2 case. We now easily derive the *Lagrange* and *Cauchy Theorems* for all finite commutative A-loops (Theorem 7.2).

Finally, in §8 we state two open problems. The first, which we expect will generate a great deal of interest in loop theory, is whether there exists a nonassociative, finite simple commutative A-loop (Problem 8.1). The results in this paper already tell us a great deal about the structure such a loop must have. The second problem (Problem 8.2) is whether every commutative A-loop of odd prime power order has a nontrivial center, that is, whether the loop is centrally nilpotent.

We should note that the variety of commutative A-loops is vast compared to the variety of abelian groups. There exist many nonassociative examples, even under very restrictive conditions such as in the case of commutative A-loops of exponent 2. While every A-loop of prime order p is isomorphic to the cyclic group of order p, a class of nonassociative commutative A-loops of order pq ($2 < p < q$ primes) was found by Drápal [7]. A survey of known constructions and the classification of commutative A-loops of small orders will appear in the planned sequel [11] to this paper. In [11], we will also give an example of a commutative A-loop of order 16 that is not centrally nilpotent.

The main idea of this paper is to associate a new loop operation with the original loop. In the odd order case, where the original loop is uniquely 2-divisible, this is a familiar approach [10], [8]. However, in all earlier instances it was somewhat transparent what the associated loop operation should be, unlike here. A common feature is to take advantage of the unique square roots. We do not have access to square roots in 2-loops, but if for every x, y there is z such that $x^2y^2 = z^2$ (Theorem 4.1), our novel idea is to declare z to be a new product of x and y. As demonstrated in this paper, this approach is most fruitful in the case of commutative A-loops. Moreover, we now have some anecdotal evidence that the connection is more profound and that binary operations associated in this or a similar manner are deserving of a systematic investigation in other varieties of loops.

The well-behaved structure theory of commutative A-loops belies the rather technical lemmas on which it is based. Most of these lemmas involve detailed equational reasoning, often obtained with the assistance of the automated theorem prover Prover9 [15].

Finally, we should mention that many of our structural results for commutative A-loops of odd order can be generalized to the noncommutative case. These generalizations will appear elsewhere [14].

1.1. **Notation.** Throughout the paper, let Q denote a commutative loop with multiplication denoted by juxtaposition and with neutral element 1. Since all left translations are bijections of Q, it is convenient to define the associated left division operation by

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

for all $x, y \in Q$. It will also be useful to introduce the *division permutations* $D_x : Q \to Q$, $x \in Q$, defined by

$$yD_x = y\backslash x = xL_y^{-1}$$

for all $x, y \in Q$. Note that $D_x^2 = \mathrm{id}_Q$ for all $x \in Q$. We will use the usual notation $x^{-1} = x\backslash 1$ for the inverse of x, and we will also use the *inversion permutation* $J : Q \to Q$ defined by

$$xJ = xD_1 = x^{-1}$$

for all $x \in Q$.

To avoid excessive parenthesization, we will use the following convention. The multiplication operation $\cdot$ will be less binding than left division, which is, in turn, less binding than juxtaposition. For example, with this convention, $ab\backslash cd \cdot g\backslash ef$ is unambiguously read as $((ab)\backslash(cd))(g\backslash(ef))$. On the other hand, we shall certainly use parentheses, brackets, etc., whenever they help to clarify an expression.

It is well known [5] that for commutative loops, the inner mapping group $\mathrm{Inn}(Q)$ has a distinguished set of generators

$$L_{x,y} = L_x L_y L_{yx}^{-1}$$

for $x, y \in Q$. Using these generators, the A-loop condition can be expressed as follows:

$$(uv)L_{x,y} = uL_{x,y} \cdot vL_{x,y}\,. \tag{A}$$

It follows from (A) that $(u\backslash v)L_{x,y} = uL_{x,y}\backslash vL_{x,y}$ and also $JL_{x,y} = L_{x,y}J$.

The assertion that a permutation φ of a loop Q is an automorphism of Q can be expressed in equivalent ways in terms of the various loop permutations:

$$L_x\varphi = \varphi L_{x\varphi}, \qquad D_x\varphi = \varphi D_{x\varphi}\,.$$

We shall use these in calculations while referencing (A).

2. Preliminaries

In this section, we establish several preliminary results for commutative A-loops which will be needed later. Some of these generalize rather easily to arbitrary A-loops, and some of those generalizations can be found in [6]. We give brief proofs in the commutative case to make the paper self-contained.

For an automorphism φ of a loop Q, let $\mathrm{Fix}(\varphi) = \{x \in Q \,|\, x\varphi = x\}$. We begin with an easy observation.

Lemma 2.1. *Let Q be a loop and let $\varphi \in \mathrm{Aut}(Q)$. Then*

(i) $\mathrm{Fix}(\varphi)$ *is a subloop.*
(ii) *If $x \in \mathrm{Fix}(\varphi)$, then $\langle x\rangle \le \mathrm{Fix}(\varphi)$.*
(iii) *For each $x \in \mathrm{Fix}(\varphi)$,*

$$L_x\varphi = \varphi L_x \qquad \text{and} \qquad D_x\varphi = \varphi D_x\,. \tag{2.1}$$

Lemma 2.2. *For all x, y, z in a commutative A-loop Q,*

$$x \in \mathrm{Fix}(L_{y,z}) \quad \Leftrightarrow \quad yL_xL_z = yL_zL_x \quad \Leftrightarrow \quad z \in \mathrm{Fix}(L_{y,x})\,.$$

Proof. We have $xL_{y,z} = x$ iff $xL_yL_z = xL_{yz}$ iff $yL_xL_z = yL_zL_x$. Since this last equation is symmetric in x and z, the other equivalence follows. □

For x in a loop Q and $n \in \mathbb{Z}$, we define $x^n = 1L_x^n$. Then $x \cdot x^n = 1L_x^nL_x = 1L_x^{n+1} = x^{n+1}$ for all $n \in \mathbb{Z}$. Also, for any $\varphi \in \mathrm{Aut}(Q)$, $(x^n)\varphi = 1L_x^n\varphi = 1\varphi L_{x\varphi}^n = (x\varphi)^n$.

Lemma 2.3 ([6], Thm 2.6)**.** *In a commutative A-loop, the following identities hold for all x, y and for all $m, n \in \mathbb{Z}$:*

$$x^nL_{y,x^m} = x^n, \tag{2.2}$$

$$L_{x^m}L_{x^n} = L_{x^n}L_{x^m}, \tag{2.3}$$

$$L_{x^n}L_{y,x^m} = L_{y,x^m}L_{x^n}, \tag{2.4}$$

$$D_{x^n}L_{y,x^m} = L_{y,x^m}D_{x^n}. \tag{2.5}$$

Proof. First, we have $xL_{y,x} = xy\backslash(x \cdot yx) = xy\backslash(xy \cdot x) = x$, so that $x \in \mathrm{Fix}(L_{y,x})$. By (A) and Lemma 2.1(ii), $x^n \in \mathrm{Fix}(L_{y,x})$ for all $n \in \mathbb{Z}$. Thus by Lemma 2.2, $x \in \mathrm{Fix}(L_{y,x^n})$, and so $x^m \in \mathrm{Fix}(L_{y,x^n})$ for all $m, n \in \mathbb{Z}$ by (A) and Lemma 2.1(ii) again. This establishes (2.2), and then (2.3) follows from another application of Lemma 2.2. Finally, (2.4) and (2.5) follow from (2.2) and (2.1). □

A loop is said to be *power-associative* if for each x, the subloop $\langle x \rangle$ is a group. Power-associativity is equivalent to $x^m x^n = x^{m+n}$ for all $x \in Q$ and all $m, n \in \mathbb{Z}$.

Lemma 2.4 ([6], Thm. 2.4)**.** *Every commutative A-loop is power-associative.*

Proof. For all $m, k \in \mathbb{Z}$ and for all x,

$$x^m x^{k+1} = x^m(x^k \cdot x) \overset{(2.4)}{=} x^k(x^m \cdot x) = x^{m+1}x^k\,.$$

By an easy induction, $x^m x^{k+n} = x^{m+n}x^k$ for all $m, n, k \in \mathbb{Z}$. Taking $k = -n$, we have the desired result. □

Lemma 2.5. *In a commutative A-loop, the following identities hold:*

$$y^n L_{y,x} = (xy\backslash x)^{-n} \qquad \text{for all } n \in \mathbb{Z}\,, \tag{2.6}$$

$$xy^2 = (xy)(xy\backslash x)^{-1}\,. \tag{2.7}$$

Proof. We compute

$$y^{-n}L_{y,x} = (y^{-1})^n L_{y,x} \overset{(A)}{=} (y^{-1}L_{y,x})^n = (xy\backslash x)^n$$

and thus obtain (2.6) upon replacing n with $-n$. Finally we have

$$xy\backslash xy^2 = yL_{y,x} \overset{(2.6)}{=} (xy\backslash x)^{-1}\,,$$

which is equivalent to (2.7). □

A loop is said to have the *automorphic inverse property* (AIP) if it has two-sided inverses and satisfies

$$(xy)^{-1} = x^{-1}y^{-1} \qquad \text{or, equivalently,} \qquad L_xJ = JL_{x^{-1}} \tag{AIP}$$

for all x, y.

Lemma 2.6. *Every commutative A-loop has the AIP.*

Proof. Using the fact that $L_{x^{-1}}L_x = L_{x^{-1},x}$ is an automorphism, we compute

$$\begin{aligned}
yL_xL_{x^{-1}}J &\overset{(2.3)}{=} yL_{x^{-1}}L_xJ && \overset{(A)}{=} y^{-1}L_{x^{-1}}L_x \\
&= x^{-1}[L_{y^{-1}}L_y^{-1}][L_yL_x] && \overset{(2.3)}{=} x^{-1}L_y^{-1}[L_{y^{-1}}L_{y,x}]L_{xy} \\
&\overset{(A)}{=} x^{-1}L_y^{-1}L_{y,x}L_{y^{-1}L_{y,x}}L_{xy} && \overset{(2.6)}{=} [(xy)^{-1}\cdot(xy\backslash x)]L_{xy} \\
&= xL_{xy}^{-1}L_{(xy)^{-1}}L_{xy} && \overset{(2.3)}{=} xL_{(xy)^{-1}} \\
&= (xy)^{-1}L_x && = yL_xJL_x\,.
\end{aligned}$$

Thus $L_xL_{x^{-1}}J = L_xJL_x$ or $L_{x^{-1}}J = JL_x$. Replacing x with x^{-1}, we obtain (AIP). □

Lemma 2.7. *In a commutative A-loop, the following identities hold:*

$$L_{x,y} = L_{x^{-1},y^{-1}}, \tag{2.8}$$

$$L_{x,y} = L^{-1}_{x^{-1}\backslash y} L_x L_y, \tag{2.9}$$

$$L_{x,y} = L_y L^{-1}_{x^{-1}\backslash y} L_x, \tag{2.10}$$

$$L_{x\backslash y,x} = L_{(y\backslash x)^{-1},x}, \tag{2.11}$$

$$L^{-1}_{(x\backslash y)^{-1}\backslash x} L_{x\backslash y} = L_y^{-1} L_{y\backslash x}. \tag{2.12}$$

Proof. First, (2.8) is an easy consequence of the AIP:

$$(zL_{x,y})^{-1} \overset{\text{(AIP)}}{=} z^{-1} L_{x^{-1},y^{-1}} \overset{\text{(A)}}{=} \left(zL_{x^{-1},y^{-1}}\right)^{-1}.$$

For (2.9), we compute

$$\begin{aligned} L^{-1}_{x^{-1}\backslash y}[L_x L_y] &= [L^{-1}_{x^{-1}\backslash y} L_{x,y}] L_{yx} && \overset{\text{(A)}}{=} L_{x,y} L^{-1}_{(x^{-1}\backslash y)L_{x,y}} L_{yx} \\ &\overset{(2.8)}{=} L_{x,y} L^{-1}_{(x^{-1}\backslash y)L_{x^{-1},y^{-1}}} L_{yx} && = L_{x,y} L^{-1}_{(y^{-1}x^{-1})^{-1}} L_{yx} \\ &\overset{\text{(AIP)}}{=} L_{x,y} L^{-1}_{yx} L_{yx} && = L_{x,y}. \end{aligned}$$

Next, we have

$$L_y^{-1} L_{x,y} \overset{(2.4)}{=} L_{x,y} L_y^{-1} \overset{(2.9)}{=} L^{-1}_{x^{-1}\backslash y} L_x,$$

which gives (2.10). For (2.11), we compute

$$L_{x\backslash y,x} = L^{-1}_{x\backslash y,x} L^2_{x\backslash y,x} \overset{\text{(A)}}{=} L^{-1}_{x\backslash y,x} L_{x\backslash y,x} L_{(x\backslash y)L_{x\backslash y,x},xL_{x\backslash y,x}} = L_{(y\backslash x)^{-1},x}$$

using (2.6) and (2.2). Finally, we apply (2.9) to both sides of (2.11) to get

$$L^{-1}_{(x\backslash y)^{-1}\backslash x} L_{x\backslash y} L_x = L^{-1}_{(y\backslash x)\backslash x} L_{y\backslash x} L_x.$$

Cancelling and using $(y\backslash x)\backslash x = y$, we obtain (2.12). □

Lemma 2.8. *For all x, y in a commutative A-loop,*

$$D_{x^2} = D_x J D_x, \tag{2.13}$$

$$x^2 = yD_x \cdot y^{-1} D_x, \tag{2.14}$$

$$x = y^{-1} D_{x^{-1}} \cdot yD_{x^2}. \tag{2.15}$$

Proof. For all x, y,

$$\begin{aligned} yD_{x^2} &= xL_x L_y^{-1} && = xL^{-1}_{x\backslash y}[L_{x\backslash y} L_x L^{-1}_{x\cdot x\backslash y}] && = xL^{-1}_{x\backslash y} L_{x\backslash y,x} \\ &\overset{\text{(A)}}{=} xL_{x\backslash y,x} L^{-1}_{(x\backslash y)L_{x\backslash y,x}} && \overset{(2.6)}{=} xL_{x\backslash y,x} L^{-1}_{(y\backslash x)^{-1}} && \overset{(2.2)}{=} xL^{-1}_{(y\backslash x)^{-1}} \\ &= (y\backslash x)^{-1} D_x && = yD_x J D_x. \end{aligned}$$

This establishes (2.13). Rewrite (2.13) as $JD_x = D_x D_{x^2}$ since $D_x^{-1} = D_x$. Applying this to y, we have $y^{-1}D_x = yD_xD_{x^2} = x^2 L^{-1}_{yD_x}$, which is equivalent to (2.14). Finally, rewrite (2.13) (applied to y) as $xL^{-1}_{yD_xJ} = yD_{x^2}$ or $x = yD_{x^2}L_{yD_xJ}$. Using (AIP), we obtain (2.15). □

3. Commutative A-loops of odd order

A loop is *uniquely 2-divisible* if the squaring map $x \mapsto x^2$ is a permutation. In finite, power-associative loops, being uniquely 2-divisible is equivalent to each element having odd order.

The following is well known and holds in more generality than we need here.

Lemma 3.1. *A finite, power-associative commutative loop Q is uniquely 2-divisible if and only if it has odd order.*

Proof. If Q is uniquely 2-divisible, then the inversion permutation J does not fix any nonidentity elements. Hence the set of nonidentity elements of Q has even order, and so Q has odd order.

Now assume Q has odd order, and fix $c \in Q$. By commutativity, the set $U = \{(x, y) \,|\, xy = c, x \neq y\}$ has even order. Since the set $V = \{(x, y) \,|\, xy = c\}$ has size $|Q|$, it follows that the set $U \backslash V = \{(x, x) \,|\, x^2 = c\}$ has odd order, and hence is nonempty. Thus the squaring map $x \mapsto x^2$ is surjective, and hence, by finiteness, is bijective. □

In this section we will study the structure of commutative A-loops of odd order in detail. To explain our approach, we first need a useful notion from group theory; cf. [3, 8].

A *twisted subgroup* of a group G is a subset $T \subset G$ satisfying (i) $1 \in T$, (ii) $a^{-1} \in T$ for each $a \in T$, and (iii) $aba \in T$ for each $a, b \in T$. A twisted subgroup T is uniquely 2-divisible if the restriction of the squaring map $x \mapsto x^2$ to T is a permutation.

On a uniquely 2-divisible twisted subgroup T, one can define a loop operation $\circ$ by $a \circ b = (ab^2a)^{1/2}$, where the exponent $1/2$ denotes the unique square root in T. The loop $(T, \circ)$ is then a (left) *Bol loop*, that is, it satisfies the identity $x \circ (y \circ (x \circ z)) = (x \circ (y \circ x)) \circ z$. In addition, $(T, \circ)$ satisfies (AIP); left Bol loops with (AIP) are known as left *Bruck loops*.

For some classes of loops, the multiplication groups contain natural twisted subgroups. Up until now, the only known example of this is the variety of Bol loops: for a Bol loop Q, the set $L_Q = \{L_x \,|\, x \in Q\}$ of left translations is a twisted subgroup of $\mathrm{Mlt}(Q)$. In case Q is uniquely 2-divisible, there is also a natural left Bruck loop structure on L_Q. It turns out that this Bruck loop structure can be isomorphically transferred to the underlying set Q itself, so that Q has two loop structures (which may or may not coincide); its original Bol loop structure and the transferred Bruck loop structure.

There are two things that make all of this particularly useful. The first is that uniquely 2-divisible Bruck loops are highly structured [9]. The second is that powers of elements in the two loop structures coincide. It is thus possible to prove results about the original Bol loop by using its associated Bruck loop. This idea was fruitfully exploited for Moufang loops by Glauberman [10]; for the Bol case, see [8].

We will now apply the same circle of ideas to commutative A-loops. We will start by identifying a twisted subgroup of the multiplication group of a commutative A-loop. For each x in a commutative A-loop Q, set

$$P_x = L_x L_{x^{-1}}^{-1} \overset{(2.3)}{=} L_{x^{-1}}^{-1} L_x \tag{P}$$

and let $P_Q = \{P_x \,|\, x \in Q\}$. Observe that the set P_Q trivially satisfies two of the conditions for being a twisted subgroup: $\mathrm{id}_Q = P_1 \in P_Q$, and for each $x \in Q$,

$$P_x P_{x^{-1}} = L_x L_{x^{-1}}^{-1} L_{x^{-1}} L_x^{-1} = \mathrm{id}_Q \,,$$

so that $P_x^{-1} = P_{x^{-1}} \in P_Q$.

Lemma 3.2. *For all x, y in a commutative A-loop Q,*

$$x^{-1} P_{xy} = xy^2, \tag{3.1}$$

$$L_{x^{-1}} P_{xy} = P_y L_x. \tag{3.2}$$

Proof. Applying (AIP) to (2.7) and rearranging gives (3.1). Next, for all $x, y \in Q$,

$$\begin{aligned} L_{x^{-1}} P_{xy} \; &= L_{x^{-1}} L_{(xy)^{-1}}^{-1} L_{xy} \overset{\text{(AIP)}}{=} L_{x^{-1}} L_{x^{-1}y^{-1}}^{-1} L_{xy} = L_{y^{-1}}^{-1} L_{y^{-1},x^{-1}} L_{xy} \\ &\overset{(2.8)}{=} L_{y^{-1}}^{-1} L_{y,x} L_{xy} \quad = L_{y^{-1}}^{-1} L_y L_x \qquad\qquad = P_y L_x \,. \end{aligned}$$

This proves (3.2). □

Note that (3.1) can also be obtained by applying (3.2) to $1 \in Q$.

Lemma 3.3. *For all x, y in a commutative A-loop Q,*

$$P_x P_y P_x = P_{yP_x} \,. \tag{3.3}$$

In particular, P_Q is a twisted subgroup of $\mathrm{Mlt}(Q)$.

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

$$\begin{aligned} P_x P_y P_x \quad &= P_x P_y L_x L_{x^{-1}}^{-1} \qquad &&\overset{(3.2)}{=} P_x L_{x^{-1}} P_{xy} L_{x^{-1}}^{-1} \\ &\overset{\text{(P)}}{=} L_x P_{xy} L_{x^{-1}}^{-1} \qquad &&= L_x P_{x^{-1}(x^{-1}\backslash xy)} L_{x^{-1}}^{-1} \\ &\overset{\text{(P)}}{=} L_x P_{x^{-1}\cdot yP_x} L_{x^{-1}}^{-1} \qquad &&\overset{(3.2)}{=} P_{yP_x} L_{x^{-1}} L_{x^{-1}}^{-1} \\ &= P_{yP_x} \,. \end{aligned}$$

This establishes (3.3), and the rest follows immediately. □

Lemma 3.4. *For all x in a commutative A-loop Q and for all $n \in \mathbb{Z}$,*

$$P_x^n = P_{x^n} \,. \tag{3.4}$$

Proof. We have already noted (3.4) for $n = -1$, while it is trivial for $n = 0, 1$. If (3.4) holds for some n, then

$$P_x^{n+2} = P_x P_{x^n} P_x \overset{(3.3)}{=} P_{x^n P_x} = P_{x^{n+2}} \,,$$

the last equality holding by power-associativity (Lemma 2.4). The rest follows by induction. □

In calculations, we will frequently use (3.4) without explicit reference.

Now assume Q is a uniquely 2-divisible, commutative A-loop. By (3.4), the twisted subgroup P_Q is also uniquely 2-divisible. Thus there is a natural Bruck loop operation $\circ$ on P_Q given by

$$P_x \circ P_y = (P_x P_y^2 P_x)^{1/2} \overset{(3.4)}{=} (P_x P_{y^2} P_x)^{1/2} \overset{(3.3)}{=} (P_{y^2 P_x})^{1/2} \overset{(3.4)}{=} P_{(y^2 P_x)^{1/2}} \,. \tag{3.5}$$

Thus as with uniquely 2-divisible Bol loops [8] or Moufang loops [10], we define a new binary operation (for which we will use the same symbol) on the underlying set Q by

$$x \circ y = (y^2 P_x)^{1/2} = (x^{-1} \backslash x y^2)^{1/2} . \tag{B}$$

By (3.5), the mapping $x \mapsto P_x$ is a surjective homomorphism from the magma $(Q, \circ)$ to the loop $(P_Q, \circ)$. In addition, note that this mapping is injective; indeed, if $P_x = \mathrm{id}_Q$, then $x^2 = 1P_x = 1$ so that $x = 1$. Thus $(Q, \circ)$ is isomorphic to $(P_Q, \circ)$. Therefore we have most of the following.

Lemma 3.5. *For a uniquely 2-divisible, commutative A-loop Q, $(Q, \circ)$ is a Bruck loop. Powers in Q coincide with powers in $(Q, \circ)$.*

Proof. The remaining assertion about powers follows easily from (B), the power-associativity of Q (Lemma 2.4), and an easy induction argument. □

In the finite case, we may now reap the benefits of the known structure theory of Bruck loops of odd order [9]. We will implicitly use Lemma 3.1 in what follows.

Proposition 3.6. *Let $A \leq B$ be subloops of a finite commutative A-loop Q of odd order. Then $|A|$ divides $|B|$. In particular, the order of any element of Q divides $|Q|$.*

Proof. The subloops A and B of Q yield subloops $(A, \circ)$ and $(B, \circ)$ of $(Q, \circ)$. The result then follows from [9], Corollary 4, p. 395. □

Proposition 3.7. *Let Q be a finite, commutative A-loop of odd order. If a prime p divides $|Q|$, then Q has an element of order p.*

Proof. Each of these results holds in the corresponding Bruck loop $(Q, \circ)$ [9]. □

Lemma 3.8. *Every inner mapping of a uniquely 2-divisible, commutative A-loop Q acts as an automorphism of $(Q, \circ)$.*

Proof. This is obvious from the definition of $\circ$. □

Lemma 3.9. *Let Q be a commutative A-loop of odd order. A subloop K of $(Q, \circ)$ is a subloop of Q if and only if $K\varphi = K$ for each $\varphi \in \mathrm{Inn}(Q) \cap \langle L_x : x \in K \rangle$.*

Proof. The "only if" direction is trivial, so assume the hypothesis of the converse. Fix $u, v \in K$. Note that $u^{-1}, v^{-1} \in K$, and since powers agree in $(Q, \circ)$ and Q, $v^{1/2} \in K$. Thus K also contains

$$(u \circ v^{1/2})^2 = v L_u L_{u^{-1}}^{-1} = v L_u^2 L_u^{-1} L_{u^{-1}}^{-1} = v L_u^2 L_{u^{-1},u}^{-1} .$$

By hypothesis, K then also contains vL_u^2. By induction, K contains vL_u^{2k} for all integers k. Now let $2n+1$ be the order of u. Then $L_u^{2n+1} \in \mathrm{Inn}(Q)$, since $1L_u^{2n+1} = u^{2n+1} = 1$. Hence K contains $vL_u^{-2n} L_u^{2n+1} = uv$, and also $vL_u^{2(-n-1)} L_u^{2n+1} = u \backslash v$. Thus K is closed under multiplication and left division in Q, and it is therefore a subloop of Q. □

At a particular point in the proof of Theorem 3.12 below, we will show that the Bruck loop associated to a certain commutative A-loop is commutative. In order to proceed, we will then need the corollary to the following technical lemma.

Lemma 3.10. *Let Q be a commutative A-loop and assume that the identity*

$$y^2P_x = x^2P_y \tag{3.6}$$

holds for all $x, y \in Q$. Then for all $x, y \in Q$,

$$y^2P_x = x^2y^2\,. \tag{3.7}$$

Corollary 3.11. *Let Q be a uniquely 2-divisible, commutative A-loop. Then $(Q, \circ)$ is commutative if and only if $(Q, \circ)$ is isomorphic to Q.*

Indeed, in the uniquely 2-divisible case, (3.6) asserts that $(Q, \circ)$ is commutative, and (3.7) says that $(x \circ y)^2 = x^2y^2$, that is, the squaring map $x \mapsto x^2$ is an isomorphism from $(Q, \circ)$ to Q.

Proof of Lemma 3.10. First we establish

$$(xy^2)P_x = xP_{xy} \tag{3.8}$$

for all $x, y \in Q$. Indeed, we have

$$\begin{aligned}(xy^2)P_x &\overset{(2.3)}{=} y^2P_xL_x \quad \overset{(3.6)}{=} x^2P_yL_x \quad \overset{(P)}{=} 1P_xP_yP_xL_{x^{-1}} \overset{(3.3)}{=} 1P_{yP_x}L_{x^{-1}}\\ &= x^{-1}\left(yP_x\right)^2 \overset{(3.1)}{=} xP_{x^{-1}\cdot yP_x} \overset{(P)}{=} xP_{xy}\,.\end{aligned}$$

Next, we will also require

$$x^{-1}P_{y^2} = y^2P_{x^{-1}}P_yL_x \tag{3.9}$$

for all $x, y \in Q$. For this, we compute

$$\begin{aligned}x^{-1}P_{y^2} &= x^{-1}P_{x\cdot x\backslash y^2} && \overset{(3.1)}{=} x(x\backslash y^2)^2\\ &= (x\backslash y^2)^2P_{y^{-1}}P_yL_x && \overset{(3.6)}{=} y^{-2}P_{x\backslash y^2}P_yL_x\\ &= \left((x\backslash y^2)\cdot(x\backslash y^2)^{-1}\backslash y^{-2}\right)P_yL_x && \overset{(AIP)}{=} \left((x\backslash y^2)\cdot(x^{-1}\backslash y^{-2})\backslash y^{-2}\right)P_yL_x\\ &= \left((x\backslash y^2)x^{-1}\right)P_yL_x && = y^2P_{x^{-1}}P_yL_x\,.\end{aligned}$$

Now, we compute

$$\begin{aligned}y^2P_xP_yL_x &\overset{(3.6)}{=} x^2P_y^2L_x && \overset{(P)}{=} 1P_xP_{y^2}P_xL_{x^{-1}}\\ &\overset{(3.3)}{=} 1P_{y^2P_x}L_{x^{-1}} && = x^{-1}\left(y^2P_x\right)^2\\ &\overset{(3.1)}{=} xP_{x^{-1}\cdot y^2P_x} && = xP_{xy^2}\\ &\overset{(AIP)}{=} xP_{x^{-1}y^{-1}}P_{xy}P_{xy^2} && \overset{(3.1)}{=} \left(x^{-1}y^{-2}\right)P_{xy}P_{xy^2}\\ &\overset{(AIP)}{=} (xy^2)^{-1}P_{xy^2\cdot(xy^2\backslash xy)}P_{xy^2} && \overset{(3.1)}{=} \left(xy^2\cdot(xy^2\backslash xy)^2\right)P_{xy^2}\\ &\overset{(3.8)}{=} (xy^2)P_{xy^2\cdot(xy^2\backslash xy)} && = (xy^2)P_{xy}\\ &\overset{(3.1)}{=} x^{-1}P_{xy}^2 && = x^{-1}P_{(xy)^2}\\ &\overset{(3.9)}{=} (xy)^2P_{x^{-1}}P_{xy}L_x\,.\end{aligned}$$

Cancelling L_x, we have

$$y^2P_xP_y = (xy)^2P_{x^{-1}}P_{xy} = 1P_{xy}P_{x^{-1}}P_{xy} = 1P_{x^{-1}P_{xy}} \overset{(3.1)}{=} 1P_{xy^2} = (xy^2)^2\,.$$

Thus

$$y^2 P_x = (xy^2)^2 P_{y^{-1}} \overset{(3.6)}{=} y^{-2} P_{y^2 x} \overset{(3.1)}{=} y^2 x^2 ,$$

which is (3.7). □

We now turn to the main result of this section

Theorem 3.12 (Odd Order Theorem)**.** *Every commutative A-loop of odd order is solvable.*

Proof. Let Q be a minimal counterexample. Since normal subloops and quotients of commutative A-loops of odd order also have odd order, it follows that Q must be simple. Let N denote the derived subloop of $(Q, \circ)$, that is, the smallest normal subloop of $(Q, \circ)$ such that $(Q/N, \circ)$ is an abelian group. Finite Bruck loops of odd order are solvable ([10], Thm. 14(b)), and so N is a proper subloop. Clearly N is fixed by every automorphism of $(Q, \circ)$. By Lemma 3.8, N is fixed by every element of $\mathrm{Inn}(Q)$. Thus by Lemma 3.9, N is a subloop of Q itself. Since N is invariant under $\mathrm{Inn}(Q)$, N is normal in Q. But Q is simple, and so $N = \{1\}$. Therefore $(Q, \circ)$ is an abelian group. By Corollary 3.11, $(Q, \circ)$ is isomorphic to Q. Thus Q is an abelian group, which contradicts the assumption that Q is not solvable. □

4. Squares and an associated loop

In an abelian group, or even a commutative Moufang loop, the product of two squares is trivially a square, for in such loops the identity $x^2y^2 = (xy)^2$ holds. This identity does not hold in commutative A-loops. For example, there is a nonassociative, commutative A-loop of order 15 ([7]) in which the identity fails. Nevertheless, the more fundamental assertion about the product of two squares holds, as we are going to show.

Motivated by Theorem 4.1 below, we introduce a new binary operation in commutative A-loops:

$$(\diamond) \qquad x \diamond y = (xy\backslash x \cdot yx\backslash y)^{-1} = yL_{y,x} \cdot xL_{x,y} ,$$

where the second equality follows from (2.6) and (AIP).

Theorem 4.1. *For all x, y in a commutative A-loop,*

$$x^2y^2 = (x \diamond y)^2 .$$

To establish the theorem, we require a few lemmas.

Lemma 4.2. *For all x, y in a commutative A-loop Q,*

$$x \diamond y = x^2 \cdot x\backslash(xy\backslash x)^{-1} . \tag{4.1}$$

Proof. First, we have

$$xL_{x,y} = (x^2y)L_{yx}^{-1} = yL_x^{-1}L_xL_{x^2}L_{yx}^{-1} \overset{(2.3)}{=} yL_x^{-1}L_{x^2}L_xL_{yx}^{-1} = yL_x^{-1}L_{x^2}L_y^{-1}L_{y,x} . \tag{4.2}$$

Thus,

$$\begin{aligned} x\diamond y &= yL_{y,x}\cdot xL_{x,y} && \overset{(4.2)}{=} yL_{y,x}\cdot yL_x^{-1}L_{x^2}L_y^{-1}L_{y,x}\\ &\overset{(A)}{=} [y\cdot yL_x^{-1}L_{x^2}L_y^{-1}]L_{y,x} && = yL_x^{-1}L_{x^2}L_{y,x}\\ &\overset{(2.1)}{=} yL_{y,x}L_x^{-1}L_{x^2} && \overset{(2.6)}{=} (xy\backslash x)^{-1}L_x^{-1}L_{x^2}\\ &= x^2\cdot x\backslash(xy\backslash x)^{-1}, \end{aligned}$$

which gives (4.1). □

Lemma 4.3. *For all x, y in a commutative A-loop,*

$$x^{-1}\backslash(xy\backslash x) = y\backslash(yx\backslash y)^{-1}. \tag{4.3}$$

Proof. We compute

$$\begin{aligned} (y\backslash(yx\backslash y)^{-1})L_{x^{-1}}L_{xy} &= (yx\backslash y)^{-1}L^{-1}_{x\backslash xy}L_{x^{-1}}L_{xy} && \overset{(2.9)}{=} (yx\backslash y)^{-1}L_{x^{-1},xy}\\ &\overset{(A)}{=} \big((xy)L_{x^{-1},xy}\backslash yL_{x^{-1},xy}\big)^{-1} && \overset{(2.2)}{=} \big(xy\backslash yL_{x^{-1},xy}\big)^{-1}\\ &\overset{(2.8)}{=} \big(xy\backslash yL_{x,(xy)^{-1}}\big)^{-1} && = \big(xy\backslash(x(xy)^{-1})^{-1}\big)^{-1}\\ &\overset{(AIP)}{=} \big(xy\backslash(x^{-1}\cdot xy)\big)^{-1} && = x. \end{aligned}$$

Thus $y\backslash(yx\backslash y)^{-1} = xL^{-1}_{xy}L^{-1}_{x^{-1}} = x^{-1}\backslash(xy\backslash x)$, as claimed. □

Now we turn to the main result of this section.

Proof of Theorem 4.1. Set $z = x\diamond y$. Then

$$\begin{aligned} x^2D_z &= zL^{-1}_{x^2} && \overset{(4.1)}{=} (x^2\cdot x\backslash(xy\backslash x)^{-1})L^{-1}_{x^2}\\ &= x\backslash(xy\backslash x)^{-1} && \overset{(AIP)}{=} (x^{-1}\backslash(xy\backslash x))J\\ &\overset{(4.3)}{=} (y\backslash(yx\backslash y)^{-1})J && = (y^2\cdot y\backslash(yx\backslash y)^{-1})L^{-1}_{y^2}J\\ &\overset{(4.1)}{=} zL^{-1}_{y^2}J && = y^2D_zJ. \end{aligned}$$

Thus $x^2 = x^2D_z^2 = y^2D_zJD_z \overset{(2.13)}{=} y^2D_{z^2} = z^2L^{-1}_{y^2}$, and so $x^2y^2 = z^2$, as claimed. □

As the notation suggests, we will now consider $(Q,\diamond)$ as being a new magma constructed on a commutative A-loop Q. We introduce notation for the corresponding left translation map:

$$yS_x = x\diamond y \tag{S}$$

for all x, y. Note that

$$S_x = L_xD_xJL_x^{-1}L_{x^2} \tag{4.4}$$

by Lemma 4.2.

Proposition 4.4. *Let Q be a commutative A-loop and let $\diamond$ be defined by $(\diamond)$. Then $(Q,\diamond)$ is a power-associative, commutative loop with the same neutral element as Q. Powers in $(Q,\diamond)$ coincide with powers in Q.*

Proof. Commutativity is clear from the definition, as is the fact that $(Q, \diamond)$ has the same neutral element as Q. By (4.4), each S_x is a permutation of Q. Hence $(Q, \diamond)$ is a loop. Finally, power-associativity of $(Q, \diamond)$ and the coinciding of powers follow from the power-associativity of Q (Lemma 2.4). □

For later use, we note the following.

Lemma 4.5. *For all x, y in a commutative A-loop Q and all $m, n \in \mathbb{Z}$,*

$$S_{x^n} L_{y,x^m} = L_{y,x^m} S_{x^n} . \tag{4.5}$$

Proof. This follows immediately from (4.4), (2.4), (2.5) and (AIP). □

We conclude this section by noting that for uniquely 2-divisible, commutative A-loops, the loop operation $\diamond$ gives nothing new.

Lemma 4.6. *If Q is a uniquely 2-divisible, commutative A-loop, then $(Q, \diamond)$ is isomorphic to Q.*

Proof. Indeed, the conclusion of Theorem 4.1 shows that the squaring map is an isomorphism from $(Q, \diamond)$ to Q. □

We will return to the associated loop operation $(Q, \diamond)$ in §6 when we consider commutative A-loops of exponent 2.

5. The Decomposition Theorem

Our main goal in this section is the following.

Theorem 5.1 (Decomposition for finite commutative A-loops)**.** *If Q is a finite commutative A-loop, then $Q = K(Q) \times H(Q)$, where $K(Q) = \{x \in Q \,|\, |x| \text{ is odd}\}$ and $H(Q) = \{x \in Q \,|\, x^{2^n} = 1 \text{ for some } n \in \mathbb{Z}\}$.*

In addition, $K(Q)$ has odd order (Theorem 5.3(v) below), and we will show later that $H(Q)$ has order a power of 2 (Theorem 7.1).

Proposition 5.2. *In a commutative A-loop Q, the set $K_1(Q) = \{x^2 \,|\, x \in Q\}$ is a normal subloop of Q.*

Proof. The set K_1 is closed under multiplication by Theorem 4.1. By Proposition 4.4, given $x, z \in Q$, there exists a unique $y \in Q$ such that $x \diamond y = z$, and so $x^2 y^2 = z^2$ by Theorem 4.1 once more. Thus K_1 is a subloop of Q. The normality of K_1 follows from the fact that all inner mappings of Q are automorphisms of Q and hence preserve squares. □

Theorem 5.3. *Let Q be a commutative A-loop. For $n \geq 1$, define*

$$K_n(Q) = \{x^{2^n} \,|\, x \in Q\},$$
$$K(Q) = \bigcap_{n \geq 1} K_n(Q).$$

Then:

(i) $K_{n+1}(Q) = \{x^2 \,|\, x \in K_n(Q)\}$ *for every* $n \geq 0$.
(ii) $K_{n+1}(Q) \subseteq K_n(Q)$ *for every* $n \geq 0$.
(iii) $K_n(Q) \trianglelefteq Q$ *for every* $n \geq 0$.
(iv) $K(Q) \trianglelefteq Q$.
(v) *If Q is finite, then $K(Q) = \{x \in Q \,|\, |x| \text{ is odd}\}$ and $|K(Q)|$ is odd.*

Proof. If $x \in K_n(Q)$, then $x = y^{2^n}$ for some $y \in Q$ and $x^2 = y^{2^{n+1}} \in K_{n+1}(Q)$. Conversely, if $x \in K_{n+1}(Q)$, then $x = z^{2^{n+1}} = (z^{2^n})^2$ for some $z \in Q$ and $z^{2^n} \in K_n(Q)$. This proves (i) and (ii).

By Proposition 5.2, $K_1(Q) \leq Q$. Assume that $K_n(Q) \leq Q$. By (i), Proposition 5.2 applied to $K_n(Q)$ yields $K_{n+1}(Q) \leq K_n(Q) \leq Q$. The normality of $K_n(Q)$ in the A-loop Q follows for free. This proves (iii) and (iv).

For (v), assume that Q is finite. Then there is n such that $K_{n+1}(Q) = K_n(Q) = K(Q) = \{x^2 \,|\, x \in K(Q)\}$, by (i). The mapping $x \mapsto x^2$ is a bijection of $K(Q)$ fixing $1 \in K(Q)$, so $K(Q)$ contains no elements of order 2 and hence no elements of even order. Conversely, pick $x \in Q$ of odd order, say $|x| = 2m+1$. The equality $x = x^{2m+2} = (x^{m+1})^2$ then implies $x \in K_1(Q)$, so that $x^{m+1} \in K_1(Q)$ by (iii). Thus $x \in K_2(Q)$ by (i), and so on, proving $x \in K(Q)$. The remaining assertion follows from Lemma 3.1. □

Lemma 5.4. *For every x, y in a commutative A-loop Q,*

$$(x\backslash(y\backslash x))^2\backslash(y^{-1}(y\backslash x))^2 = (x\backslash y)^{-2}. \tag{5.1}$$

Proof. With y replaced by $x\backslash y$, (2.7) yields

$$x(x\backslash y)^2 = y(y\backslash x)^{-1}\,. \tag{5.2}$$

Replacing y with $y\backslash x$ and using $(y\backslash x)\backslash x = y$ gives

$$x(x\backslash(y\backslash x))^2 = y^{-1}(y\backslash x)\,. \tag{5.3}$$

Applying J and using (AIP) gives

$$x^{-1}(x\backslash(y\backslash x))^{-2} = y(y\backslash x)^{-1}\,. \tag{5.4}$$

Putting (5.2) and (5.4) together, we have

$$(x\backslash y)^2(x\backslash(y\backslash x))^{-2} = xD_{y(y\backslash x)^{-1}} \cdot x^{-1}D_{y(y\backslash x)^{-1}} \overset{(2.14)}{=} (y(y\backslash x)^{-1})^2\,.$$

Applying J to both sides and using (AIP), we have

$$(x\backslash y)^{-2}(x\backslash(y\backslash x))^2 = (y^{-1}(y\backslash x))^2,$$

and this is clearly equivalent to (5.1). □

Proposition 5.5. *Let Q be a commutative A-loop, and let $x \in Q$ satisfy $x^{2^n} = 1$. Then $(xy)^{2^n} = y^{2^n}$ for every $y \in Q$.*

Proof. We proceed by induction on n. The claim is clearly true when $n = 0$. Let $n \geq 0$, assume that the claim holds for n, and let $x \in Q$ satisfy $x^{2^{n+1}} = 1$. Then the induction assumption yields

$$(x^2y)^{2^n} = y^{2^n} = (x^2(x^2\backslash y))^{2^n} = (x^2\backslash y)^{2^n} \tag{5.5}$$

for every $y \in Q$. We may apply any automorphism φ to (5.5), and then set $z = y\varphi$ to obtain $((x\varphi)^2z)^{2^n} = z^{2^n} = ((x\varphi)^2\backslash z)^{2^n}$ for all $z \in Q$. In particular, we choose $\varphi = JL_{x,x\backslash y}$ (by (A) and (AIP)). Then $xJL_{x,x\backslash y} = y\backslash(x\backslash y)$ by (2.6) (or direct calculation). Hence

$$(z(y\backslash(x\backslash y))^2)^{2^n} = z^{2^n} = ((y\backslash(x\backslash y))^2\backslash z)^{2^n} \tag{5.6}$$

for every $y, z \in Q$. Thus

$$y^{2^{n+1}} \overset{(5.6)}{=} [y(y\backslash(x\backslash y))^2]^{2^{n+1}} \overset{(5.3)}{=} [x^{-1}(x\backslash y)]^{2^{n+1}} = [(x^{-1}(x\backslash y))^2]^{2^n}$$
$$\overset{(5.6)}{=} [(y\backslash(x\backslash y))^2\backslash(x^{-1}(x\backslash y))^2]^{2^n} \overset{(5.1)}{=} (y\backslash x)^{-2^{n+1}}.$$

Then

$$(y^{-1})^{-2^{n+1}} = y^{2^{n+1}} \overset{(2.2)}{=} y^{2^{n+1}} L_{y,y^{-1}} = (y\backslash x)^{-2^{n+1}} L_{y,y^{-1}}$$
$$\overset{(A)}{=} ((y\backslash x)L_{y,y^{-1}})^{-2^{n+1}} = (y^{-1}x)^{-2^{n+1}}.$$

Taking inverses and replacing y with y^{-1}, we obtain $y^{2^{n+1}} = (xy)^{2^{n+1}}$, which completes the proof. □

Theorem 5.6. *Let Q be a commutative A-loop. For $n \geq 0$, let*

$$H_n(Q) = \{x \in Q \mid x^{2^n} = 1\},$$
$$H(Q) = \bigcup_{n \geq 0} H_n(Q).$$

Then:

(i) $H_{n+1}(Q) = \{x \in Q \mid x^2 \in H_n(Q)\}$ *for every* $n \geq 0$.
(ii) $H_{n+1}(Q) \supseteq H_n(Q)$ *for every* $n \geq 0$.
(iii) $H_n(Q) \trianglelefteq Q$ *for every* $n \geq 0$.
(iv) $H(Q) \trianglelefteq Q$.

Proof. Parts (i) and (ii) are obvious. For (iii) and (iv), it suffices to show that $H_n(Q) \leq Q$ for every $n \geq 0$ and $H(Q) \leq Q$. Let $x \in H_n(Q)$, $y \in H_m(Q)$ and let $k = \max\{n, m\}$. Then Proposition 5.5 yields $(xy)^{2^k} = x^{2^k} = 1$ and $(x\backslash y)^{2^k} = (x \cdot x\backslash y)^{2^k} = y^{2^k} = 1$. □

Finally, we turn to the proof of the main result of this section.

Proof of Theorem 5.1. By Theorems 5.3 and 5.6, K and H are normal subloops of Q. Clearly $K \cap H = 1$, and $KH = Q$ is proved in the same way as for groups (since the argument takes place in cyclic subgroups, by power-associativity). Then $Q = K \times H$ follows. □

6. Commutative A-loops of exponent 2

We now turn to commutative A-loops of exponent 2. The following result shows why this special case is of particular importance.

Proposition 6.1. *A finite simple commutative A-loop is either a cyclic group of order p for some odd prime p, or it has exponent* 2.

Proof. Let Q be a finite simple commutative A-loop. By the Decomposition Theorem 5.1, $Q = K(Q) \times H(Q)$. Since Q is simple, $Q = K(Q)$ or $Q = H(Q)$. In the former case, Q is solvable by Theorems 5.3(v) and 3.12. Thus Q is both simple and solvable, and hence is a cyclic group of odd prime order. Now assume $Q = H(Q)$, that is, every element of Q has order a power of 2. The subloop $K_1(Q) = \{x^2 \mid x \in Q\}$ is normal (Proposition 5.2), and so either $K_1(Q) = Q$ or $K_1(Q) = \langle 1 \rangle$. In the former case, the squaring map is a bijection by finiteness,

but then Q has odd order by Lemma 3.1, a contradiction. Thus for every $x \in Q$, $x^2 = 1$, that is, Q has exponent 2. □

Our goal in this section is to establish the following.

Theorem 6.2. *Let Q be a commutative A-loop of exponent 2. Then $(Q, \diamond)$ is an elementary abelian 2-group.*

Corollary 6.3. *If Q is a finite, commutative A-loop of exponent 2, then $|Q|$ is a power of 2.*

The proof of Theorem 6.2 will require some technical lemmas. *Throughout the rest of this section*, let Q be a commutative A-loop of exponent 2. The operation $\diamond$ and the corresponding translations S_x simplify accordingly:

$$x \diamond y = x\backslash(xy\backslash x),$$
$$S_x = L_x D_x L_x^{-1}.$$

Thus $S_x^2 = L_x D_x L_x^{-1} L_x D_x L_x^{-1} = L_x D_x^2 L_x^{-1} = \mathrm{id}_Q$. This establishes the following.

Lemma 6.4. *For all $x, y \in Q$, $x \diamond (x \diamond y) = y$, that is, $S_x^2 = \mathrm{id}_Q$.*

Lemma 6.5. *For all $x \in Q$,*

$$S_x = L_x D_x L_x^{-1} = L_x^{-1} D_x L_x\,. \tag{6.1}$$

Proof. The first equality has already been established. Since Q has exponent 2, $D_x = D_{xL_x^2}$ for each x. Now $L_x^2 = L_{x,x} \in \mathrm{Inn}(Q)$, and so we have $L_x^2 D_x = L_x^2 D_{xL_x^2} \overset{(A)}{=} D_x L_x^2$. Applying L_x^{-1} on the left and on the right, we obtain the desired result. □

Lemma 6.6. *For all $x, y, z \in Q$,*

$$yL_{z\backslash(x\cdot zy),z} S_{zy} = zL_y L_x^{-1} D_y L_x\,. \tag{6.2}$$

Proof. First, we compute

$$\begin{aligned}
&yL_{x,z}S_{zy}L_{zx\backslash zy}^{-1}L_{zx}\\
&\quad = yL_{x,z}S_{zy}L_{zy}^{-1}[L_{zy}L_{zx\backslash zy}^{-1}L_{zx}] && \overset{(2.10)}{=} yL_{x,z}S_{zy}[L_{zy}^{-1}L_{zx,zy}]\\
&\quad \overset{(2.4)}{=} yL_{x,z}[S_{zy}L_{zx,zy}]L_{zy}^{-1} && \overset{(4.5)}{=} y[L_{x,z}L_{zx,zy}]S_{zy}L_{zy}^{-1}\\
&\quad = [yL_x]L_z[L_{zx}^{-1}L_{zx}]L_{zy}L_{zy\cdot zx}^{-1}S_{zy}L_{zy}^{-1} && = xL_yL_zL_{zy}L_{zy\cdot zx}^{-1}[S_{zy}L_{zy}^{-1}]\\
&\quad \overset{(6.1)}{=} xL_yL_zL_{zy}L_{zy\cdot zx}^{-1}L_{zy}^{-1}D_{zy}\,.
\end{aligned}$$

Now since Q has exponent 2, $1L_yL_zL_{zy} = 1$, and so $L_yL_zL_{zy} \in \mathrm{Inn}(Q)$. Also, $zx \cdot zy = (y\backslash x)L_yL_zL_{zy}$. Thus we may apply (A) to get

$$\begin{aligned}
yL_{x,z}S_{zy}L_{zx\backslash zy}^{-1}L_{zx} &= xL_{y\backslash x}^{-1}L_yL_z[L_{zy}L_{zy}^{-1}]D_{zy} = [xL_{y\backslash x}^{-1}]L_yL_zD_{zy}\\
&= [yD_x^2L_yL_z]D_{zy} && = zD_{zy}\\
&= y,
\end{aligned}$$

where we have used $y^2 = 1$ in the penultimate step. Hence

$$yL_{x,z}S_{zy} = yL_{zx}^{-1}L_{zx\backslash zy} \overset{(2.12)}{=} yL_{(zy\backslash zx)\backslash zy}^{-1}L_{zy\backslash zx}\,.$$

Replacing x with $xL_{zy}L_z^{-1} = z\backslash(x \cdot zy)$, we obtain

$$yL_{z\backslash(x\cdot zy),z}S_{zy} = yL_{x\backslash zy}^{-1}L_x = zL_yL_x^{-1}D_yL_x\,.$$

This establishes (6.2). □

Lemma 6.7. *For all $u, v, w \in Q$,*

$$uL_{v\backslash(w\cdot uv),v} = uL_vL_w^{-1}D_vL_w\,. \tag{6.3}$$

Proof. We compute

$$\begin{aligned}
uL_{v\backslash(w\cdot uv),v} &= [uL_{v\backslash(w\cdot uv)}]L_vL_{w\cdot uv}^{-1} && = w[L_{uv}L_v^{-1}L_u]L_vL_{w\cdot uv}^{-1}\\
&\overset{(2.10)}{=} wL_{u,uv}L_vL_{w\cdot uv}^{-1} && = wL_{v\backslash uv,uv}L_vL_{w\cdot uv}^{-1}\\
&\overset{(2.11)}{=} w[L_{uv\backslash v,uv}L_v]L_{w\cdot uv}^{-1} && = [wL_{uv\backslash v}]L_{uv}L_{w\cdot uv}^{-1}\\
&= (uv\backslash v)L_wL_{uv}L_{w\cdot uv}^{-1} && = vL_{uv}^{-1}L_{w,uv}\\
&\overset{(2.10)}{=} vL_{w\backslash uv}^{-1}L_w && = uL_vL_w^{-1}D_vL_w\,,
\end{aligned}$$

which establishes (6.3). □

Lemma 6.8. *For all $u, v, w \in Q$,*

$$uL_{v\backslash w}^{-1}L_vL_{vw,u} = wu\,. \tag{6.4}$$

Proof. We compute

$$\begin{aligned}
u[L_{v\backslash w}^{-1}L_v]L_{vw,u} &\overset{(2.9)}{=} uL_{v,w}L_w^{-1}L_{vw,u} && \overset{(2.4)}{=} uL_w^{-1}[L_{v,w}L_{vw,u}]\\
&= [uL_w^{-1}L_v]L_wL_uL_{vw\cdot u}^{-1} && = vL_{w\backslash u}L_wL_uL_{vw\cdot u}^{-1}\\
&= v[L_{w\backslash u}L_{w,u}]L_{wu}L_{vw\cdot u}^{-1} && \overset{(2.9)}{=} vL_wL_uL_{wu}L_{vw\cdot u}^{-1}\\
&= ((u\cdot vw)\cdot wu)L_{vw\cdot u}^{-1} && = wu\,,
\end{aligned}$$

which establishes (6.4). □

Lemma 6.9. *For all $u, v, w \in Q$,*

$$vL_{w,u}S_{uv} = vL_{w,u}L_u^{-1}L_v\,. \tag{6.5}$$

Proof. We begin with

$$vL_{u\backslash(w\cdot uv),u}S_{uv} \overset{(6.2)}{=} uL_vL_w^{-1}D_vL_w \overset{(6.3)}{=} uL_{v\backslash(w\cdot vu),v}\,.$$

Replacing w with $wL_{uv}^{-1}L_u$, we have

$$\begin{aligned}
vL_{w,u}S_{uv} &= uL_{v\backslash uw,v} && \overset{(2.11)}{=} uL_{uw\backslash v,v}\\
&\overset{(2.9)}{=} uL_{(uw\backslash v)\backslash v}^{-1}L_{uw\backslash v}L_v && = uL_{uw}^{-1}L_{uw\backslash v}L_v\\
&= vL_{uw}^{-1}L_{uw\backslash u}L_v && \overset{(2.12)}{=} vL_{(u\backslash uw)\backslash u}^{-1}L_{u\backslash uw}L_v\\
&= vL_{w\backslash u}^{-1}L_wL_v && \overset{(2.9)}{=} vL_{w,u}L_u^{-1}L_v\,.
\end{aligned}$$

This establishes (6.5). □

Lemma 6.10. *For all $x, y \in Q$,*

$$L_x^{-1}D_yL_x = L_y^{-1}D_xL_yD_{xy}\,. \tag{6.6}$$

Proof. We have

$$\begin{aligned} zL_yL_x^{-1}D_yL_x &\overset{(6.2)}{=} yL_{z\backslash(x\cdot zy)}S_{zy} &&\overset{(6.3)}{=} y[L_zL_x^{-1}]D_zL_xS_{zy} \\ &= yL_{z\backslash x}^{-1}[L_{z\backslash x,z}D_z]L_xS_{zy} &&\overset{(2.5)}{=} yL_{z\backslash x}^{-1}D_z[L_{z\backslash x,z}L_x]S_{zy} \\ &= yL_{z\backslash x}^{-1}D_zL_{z\backslash x}L_zS_{zy}\,. \end{aligned}$$

Now set $u = yL_{z\backslash x}^{-1}D_zL_{z\backslash x} = zL_{(z\backslash x)\backslash y}^{-1}L_{z\backslash x}$, and observe that

$$uL_{(z\backslash x)y,z} \overset{(6.4)}{=} yz\,. \tag{6.7}$$

Thus using the commutativity of $\diamond$, we compute

$$\begin{aligned} zL_yL_x^{-1}D_yL_x &= (zu)S_{zy} &&= (zy)S_{zu} &&\overset{(6.7)}{=} uL_{(z\backslash x)y,z}S_{zu} \\ &\overset{(6.5)}{=} uL_{(z\backslash x)y,z}L_z^{-1}L_u &&\overset{(6.7)}{=} (yz)L_z^{-1}L_u &&= yL_u \\ &= uL_y &&= zL_{(z\backslash x)\backslash y}^{-1}L_{z\backslash x}L_y &&\overset{(2.9)}{=} zL_{z\backslash x,y} \\ &= zL_{z\backslash x}L_yL_{(z\backslash x)y}^{-1} &&= (yx)L_{(z\backslash x)y}^{-1} &&= zD_xL_yD_{xy}\,. \end{aligned}$$

Thus $L_yL_x^{-1}D_yL_x = D_xL_yD_{xy}$. Multiplying on the left by L_y^{-1}, we obtain (6.6). □

Lemma 6.11. *For all $x, y \in Q$,*

$$L_x^{-1}D_yL_x = L_{xy}^{-1}S_{(xy)\backslash x}L_{xy}\,. \tag{6.8}$$

Proof. We compute

$$\begin{aligned} L_x^{-1}D_yL_x &= L_x^{-1}L_y^{-1}S_yL_yL_x &&= L_x^{-1}L_y^{-1}S_yL_{y,x}L_{xy} \\ &\overset{(A)}{=} L_x^{-1}L_y^{-1}L_{y,x}S_{yL_{y,x}}L_{xy} &&\overset{(2.6)}{=} L_{xy}^{-1}S_{(xy)\backslash x}L_{xy}\,, \end{aligned}$$

where we have also used the assumption that Q has exponent 2 in the last step. □

Finally, we have enough for the main result of this section.

Proof of Theorem 6.2. By commutativity of $\diamond$ (Proposition 4.4) and $x \diamond x = x^2 = 1$ for all $x \in Q$, all that is needed is to show that $\diamond$ is associative. First, apply (6.8) to both sides of (6.6) to obtain $L_{xy}^{-1}S_{(xy)\backslash x}L_{xy} = L_{yx}^{-1}S_{(yx)\backslash y}L_{yx}D_{xy}$ or $S_{(xy)\backslash x} = S_{(yx)\backslash y}L_{yx}D_{xy}L_{xy}^{-1} = S_{(yx)\backslash y}S_{xy}$. Replace x with $y\backslash x$ to get $S_{x\backslash(y\backslash x)} = S_{x\backslash y}S_x$. Replace y with xy to obtain $S_{x\backslash(xy\backslash x)} = S_yS_x$ or $S_{x\diamond y} = S_yS_x$. This is precisely associativity of $\diamond$: applying both sides to z, we have $(x \diamond y) \diamond z = x \diamond (y \diamond z)$ for all $x, y, z \in Q$. This completes the proof. □

7. p-LOOPS

For a finite, power-associative loop Q, there are at least two reasonable ways to define what it means for Q to be a *p-loop*: either every element of Q has order a power of p, or $|Q|$ is a power of p. Fortunately, these two notions are equivalent for groups, Moufang loops, and, as we are about to show, for commutative A-loops.

Theorem 7.1. *Let Q be a finite commutative A-loop and let p be a prime. Then $|Q|$ is a power of p if and only if every element of Q has order a power of p.*

Proof. Assume first that p is odd. If $|Q|$ is a power of p, then by Proposition 3.6, every element of Q has order a power of p. Conversely, if $|Q|$ is divisible by an odd prime q, then by Proposition 3.7(iii), Q contains an element of order q. Thus if every element of Q has order a power of p, $|Q|$ must be a power of p.

Now assume that $p = 2$ and that $|Q|$ is a power of 2. Since $Q = K(Q) \times H(Q)$ (Theorem 5.1) and $|K(Q)|$ is odd (Theorem 5.3), we must have $K(Q) = \langle 1 \rangle$, and so $Q = K(Q)$; that is, every element of Q has order a power of 2.

For the converse, assume that Q is a smallest commutative A-loop of exponent a power of 2 such that $|Q|$ is not a power of 2. Consider the normal subloop $1 < H_1 = \{x \in Q \,|\, x^2 = 1\}$; cf. Theorem 5.6. Then $|H_1|$ is a power of 2 by Corollary 6.3. If $H_1 = Q$, we have reached a contradiction. If $H_1 < Q$, then $|Q/H_1|$ is a power of 2 by minimality, and so $|Q| = |H_1| \cdot |Q/H_1|$ is a power of 2, a contradiction. □

Unlike in the case of abelian groups, for a finite commutative A-loop Q, the normal subloop $K(Q)$ does not necessarily decompose as a direct product of p-loops. For example, Drápal [7] constructed a commutative A-loop of order 15 that is not a direct product of a 3-loop and a 5-loop.

Theorem 7.2 (Lagrange and Cauchy Theorems)**.** *Let Q be a finite commutative A-loop. Then:*

(i) *If $x \in A \leq Q$, then both $|x|$ and $|A|$ divide $|Q|$.*
(ii) *If a prime p divides $|Q|$, then Q has an element of order p.*

Proof. Combine Theorems 5.1, 7.1 and Propositions 3.6, 3.7. □

8. Open problems

We conclude this paper with two open problems.

Problem 8.1. Does there exist a nonassociative, finite simple commutative A-loop?

By Proposition 6.1 and Corollary 6.3, such a loop would have exponent 2 and order a power of 2. To get some insight into the problem, more constructions of commutative A-loops which are 2-loops are needed; see [11].

Recall that the *center* of a loop Q is the set of all elements a satisfying $a \cdot xy = x \cdot ay = xa \cdot y$ for all x, y. In groups and Moufang loops, the center of a p-loop is always nontrivial, and thus such loops are centrally nilpotent.

Problem 8.2. Let p be an odd prime. Does there exist a finite commutative A-loop of order a power of p with trivial center?

By a classic result of Albert [1], it would be sufficient to show that $\mathrm{Mlt}(Q)$ is a p-group.

The restriction to odd p is necessary. There exist commutative A-loops of exponent 2 of all orders 2^n, $n \geq 4$, with trivial center [11].

References

[1] A. A. Albert, Quasigroups II, *Trans. Amer. Math. Soc.* **55** (1944), 401–419. MR0010597 (6:42a)
[2] M. Aschbacher, *Finite Group Theory*, Cambridge Univ. Press, Cambridge, 1986. MR895134 (89b:20001)

[3] M. Aschbacher, Near subgroups of finite groups, *J. Group Theory* **1** (1998), 113–129. MR1614316 (99e:20031)
[4] V. D. Belousov, *Foundations of the Theory of Quasigroups and Loops*, Izdat. Nauka, Moscow, 1967 (Russian). MR0218483 (36:1569)
[5] R. H. Bruck, *A Survey of Binary Systems*, Springer-Verlag, 1971. MR0093552 (20:76)
[6] R. H. Bruck and L. J. Paige, Loops whose inner mappings are automorphisms, *Ann. of Math.* (2) **63** (1956), 308–323. MR0076779 (17:943b)
[7] A. Drápal, A class of commutative loops with metacyclic inner mapping groups, *Comment. Math. Univ. Carolin.* **49** (2008), 357–382. MR2490433
[8] 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. MR2228190 (2007d:20115)
[9] G. Glauberman, On loops of odd order I, *J. Algebra* **1** (1964), 374–396. MR0175991 (31:267)
[10] G. Glauberman, On loops of odd order II, *J. Algebra* **8** (1968), 393–414. MR0222198 (36:5250)
[11] P. Jedlička, M. K. Kinyon and P. Vojtěchovský, Constructions of commutative automorphic loops, *Comm. Alg.*, to appear.
[12] T. Kepka, M. K. Kinyon and J. D. Phillips, The structure of F-quasigroups, *J. Algebra* **317** (2007), 435–461. MR2362925 (2008h:20100)
[13] M. K. Kinyon, K. Kunen and J. D. Phillips, Every diassociative A-loop is Moufang, *Proc. Amer. Math. Soc.* **130** (2002), 619–624. MR1866009 (2002k:20124)
[14] M. K. Kinyon, K. Kunen and J. D. Phillips, A generalization of Moufang loops and A-loops, in preparation.
[15] W. McCune, *Prover9*, version 2008-06A, (`http://www.cs.unm.edu/ mccune/prover9/`)
[16] J. M. Osborn, A theorem on A-loops, *Proc. Amer. Math. Soc.* **9** (1958), 347–349. MR0093555 (20:79)
[17] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math. **8**, Heldermann Verlag, Berlin, 1990. MR1125767 (93g:20132)
[18] P. Plaumann and L. Sabinina, On nuclearly nilpotent loops of finite exponent, *Comm. Alg.* **36** (2008), 1346–1353. MR2406589 (2009c:20124)

Department of Mathematics, Faculty of Engineering, Czech University of Life Sciences, Kamýcká 129, 165 21 Prague 6-Suchdol, Czech Republic
E-mail address: `jedlickap@tf.czu.cz`

Department of Mathematics, University of Denver, 2360 S Gaylord St., Denver, Colorado 80208
E-mail address: `mkinyon@math.du.edu`

Department of Mathematics, University of Denver, 2360 S Gaylord St., Denver, Colorado 80208
E-mail address: `petr@math.du.edu`