TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 368, Number 12, December 2016, Pages 8901–8927
http://dx.doi.org/10.1090/tran/6622
Article electronically published on March 21, 2016

# THE STRUCTURE OF AUTOMORPHIC LOOPS

MICHAEL K. KINYON, KENNETH KUNEN, J. D. PHILLIPS,
AND PETR VOJTĚCHOVSKÝ

Abstract. Automorphic loops are loops in which all inner mappings are automorphisms. This variety of loops includes, for instance, groups and commutative Moufang loops.

We study uniquely 2-divisible automorphic loops, particularly automorphic loops of odd order, from the point of view of the associated Bruck loops (motivated by Glauberman's work on uniquely 2-divisible Moufang loops) and the associated Lie rings (motivated by a construction of Wright). We prove that every automorphic loop $Q$ of odd order is solvable and contains an element of order $p$ for every prime $p$ dividing $|Q|$, and that $|S|$ divides $|Q|$ for every subloop $S$ of $Q$.

There are no finite simple nonassociative commutative automorphic loops, and there are no finite simple nonassociative automorphic loops of order less than 2500. We show that if $Q$ is a finite simple nonassociative automorphic loop, then the socle of the multiplication group of $Q$ is not regular. The existence of a finite simple nonassociative automorphic loop remains open.

Let $p$ be an odd prime. Automorphic loops of order $p$ or $p^2$ are groups, but there exist nonassociative automorphic loops of order $p^3$, some with trivial nucleus (center) and of exponent $p$. We construct nonassociative "dihedral" automorphic loops of order $2n$ for every $n > 2$, and show that there are precisely $p-2$ nonassociative automorphic loops of order $2p$, all of them dihedral.

## 1. Introduction

A *loop* $(Q, \cdot)$ is a set $Q$ with a binary operation $\cdot : Q \times Q \to Q$ such that (i) $(Q, \cdot)$ is a *quasigroup*; that is, for each $a$, $b \in Q$, the equations $ax = b$ and $ya = b$ have unique solutions $x$, $y \in Q$, and (ii) there exists a neutral element $1 \in Q$ such that $1x = x1 = x$ for all $x \in Q$. Equivalently, a loop can be viewed as having three binary operations $\cdot, \backslash, /$ satisfying the identities $x\backslash(xy) = y$, $x(x\backslash y) = y$, $(xy)/y = x$, $(x/y)y = x$, $x/x = y\backslash y$. Basic references for loop theory are [2, 25].

For $a \in Q$, the *right translation* and *left translation* by $a$ are the bijections $R_a : Q \to Q; x \mapsto xa$ and $L_a : Q \to Q; x \mapsto ax$. These generate the *multiplication group* $\mathrm{Mlt}(Q) = \langle R_x, L_x \mid x \in Q \rangle$. The *inner mapping group* is the subgroup stabilizing the neutral element, $\mathrm{Inn}(Q) = (\mathrm{Mlt}(Q))_1$.

A loop is *automorphic* (or an *A-loop*) if every inner mapping is an automorphism, that is, if $\mathrm{Inn}(Q) \leq \mathrm{Aut}(Q)$. The study of automorphic loops began in 1956 with Bruck and Paige [3]. They were particularly interested in *diassociative* automorphic

Received by the editors October 4, 2012 and, in revised form, November 26, 2014.
2010 *Mathematics Subject Classification.* Primary 20N05.
*Key words and phrases.* Automorphic loop, inner mapping, Odd Order Theorem, Cauchy Theorem, Lagrange Theorem, solvable loop, Bruck loop, Lie ring, middle nuclear extension, dihedral automorphic loop, simple automorphic loop, primitive group.
The fourth author was partially supported by Simons Foundation Collaboration Grant 210176.

loops, that is, loops in which each 2-generated subloop is a group. They noted that such loops share many properties with Moufang loops. Shortly thereafter, Osborn showed that commutative diassociative automorphic loops are Moufang [24]. More results showing the Moufang nature of diassociative, automorphic loops were found in [10] and [27, Thm. 5]. The general case was finally settled in [21]: Every diassociative automorphic loop is a Moufang loop.

In recent years, a detailed structure theory has emerged for *commutative* automorphic loops. For instance, the Odd Order, Lagrange and Cauchy Theorems hold for commutative automorphic loops, a finite commutative automorphic loop has order $p^k$ if and only if each element has order a power of $p$, and a finite commutative automorphic loop decomposes as a direct product of a loop of odd order and a loop of order a power of 2 [17]; there are no finite simple nonassociative commutative automorphic loops [15]; for an odd prime $p$, if $Q$ is a finite commutative automorphic $p$-loop, then $\mathrm{Mlt}(Q)$ is a $p$-group and $Q$ is centrally nilpotent [5, 19]; for an odd prime $p$, commutative automorphic loops of order $p$, $p^2$, $2p$, $2p^2$, $4p$, $4p^2$ are groups [18].

In this paper we lay foundations for the study of automorphic loops. Our understanding is not yet as complete as in the commutative case, but we obtain several significant results, as described below. For notation and terminology, see Section 2.

1.1. **Summary of results.** Section 2 introduces the notation, definitions, and preliminary results concerned mostly with identities valid in automorphic loops.

Sections 3, 4: Motivated by work of Glauberman, we first study certain derived operations on automorphic loops. In [13, 14] Glauberman showed that Bruck loops of odd order are solvable and satisfy the Cauchy, Lagrange and Sylow Theorems. He also constructed a Bruck loop $(Q, \circ)$ from a uniquely 2-divisible Moufang loop $(Q, \cdot)$ by setting $x \circ y = (xy^2x)^{1/2}$, and this allowed him to transfer the above results from Bruck loops of odd order to Moufang loops of odd order.

We show in three steps that the analog of Glauberman's operation for uniquely 2-divisible automorphic loops is the operation

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

which coincides with Glauberman's operation on Moufang loops because Moufang loops are diassociative. First, given any automorphic loop $(Q, \cdot)$, we show that the core $(Q, *)$ defined by

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

is an involutive quandle. Second, using the core, we show that the set $P_Q = \{P_x \mid x \in Q\}$ with $P_x = R_x L_{x^{-1}}^{-1}$ is a twisted subgroup of $\mathrm{Mlt}(Q)$, satisfying $P_x P_y P_y = P_{yP_x}$ and $P_x^n = P_{x^n}$. As is well known, on a uniquely 2-divisible twisted subgroup $(T, \cdot)$ one can define a Bruck loop $(T, \bullet)$ by

$$x \bullet y = (xy^2x)^{1/2}.$$

Hence, if $Q$ is uniquely 2-divisible, $(P_Q, \bullet)$ is a twisted subgroup. Third, the operation $\bullet$ can be transferred from $P_Q$ onto $Q$, yielding the associated Bruck loop $(Q, \circ)$.

A finite automorphic loop is uniquely 2-divisible if and only if it is of odd order. The above discussion therefore applies to automorphic loops of odd order, and then

results of Glauberman on Bruck loops lead to the Lagrange and Cauchy (but not Sylow) Theorems for automorphic loops of odd order.

Sections 5, 6: The next ingredient is based on Wright's construction of loops from algebras. Specializing it to a Lie ring $(Q, +, [\cdot,\cdot])$, we can define $(Q, \diamond)$ by

$$x \diamond y = x + y - [x, y].$$

Then $(Q, \diamond)$ is a loop if and only if in $(Q, +, [\cdot,\cdot])$ the mappings

$$(W_1) \qquad y \mapsto y \pm [y, x] \text{ are invertible for every } x \in Q.$$

Moreover, if $(Q, +, [\cdot,\cdot])$ is a Lie ring satisfying $(W_1)$, then a sufficient condition for $(Q, \diamond)$ to be automorphic is that

$$(W_2) \qquad [[Q, x], [Q, x]] = 1 \text{ for every } x \in Q.$$

In the uniquely 2-divisible case we obtain a correspondence: If $(Q, +, [\cdot,\cdot])$ is a uniquely 2-divisible Lie ring satisfying $(W_1)$ and $(W_2)$, then $(Q, \diamond)$ is a uniquely 2-divisible automorphic loop whose associated Bruck loop $(Q, \circ)$ is an abelian group. Conversely, if $(Q, \cdot)$ is a uniquely 2-divisible automorphic loop whose associated Bruck loop $(Q, \circ)$ is an abelian group, then $(Q, \circ, [\cdot,\cdot])$ defined by

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

(the inverses in $(Q, \cdot)$ and $(Q, \circ)$ coincide) is a Lie ring satisfying $(W_1)$ and $(W_2)$. Moreover, the two constructions are inverse to each other, subrings (resp. ideals) of the Lie ring are subloops (resp. normal subloops) of the automorphic loop, and subloops (resp. normal subloops) of the automorphic loop closed under square roots are subrings (resp. ideals) of the Lie ring.

Taking advantage of the associated Lie rings, we prove the Odd Order Theorem for automorphic loops, we show that automorphic loops of order $p^2$ are groups, and we give examples of automorphic loops of order $p^3$ with trivial nucleus.

Section 7: Next we investigate finite simple automorphic loops. Since a loop $Q$ is simple if and only if $\mathrm{Mlt}(Q)$ is a primitive permutation group on $Q$, we approach the problem from the direction of primitive groups. In [20] we proved computationally, using the library of primitive groups in GAP, that a finite simple automorphic loop of order less than 2500 is associative. Here we show that if $Q$ is a finite simple nonassociative automorphic loop, then the socle of $\mathrm{Mlt}(Q)$ is not regular. Hence, by the O'Nan-Scott theorem, $\mathrm{Mlt}(Q)$ is of almost simple type, of diagonal type or of product type. Whether such a loop exists remains open.

We also prove that characteristically simple automorphic loops behave analogously to characteristically simple groups.

Sections 8, 9: We conclude the paper with a short discussion of middle nuclear extensions and, as an application, with constructions of generalized dihedral automorphic loops. Namely, if $(A, +)$ is an abelian group and $\alpha \in \mathrm{Aut}(A)$, then $\mathbb{Z}_2 \times A$ with multiplication $(i, u)(j, v) = (i + j, ((-1)^j u + v)\alpha^{ij})$ is an automorphic loop. In particular, if $A = \mathbb{Z}_n$ and $c$ is an invertible element of $\mathbb{Z}_n$, then $\mathbb{Z}_2 \times \mathbb{Z}_n$ with multiplication $(i, u)(j, v) = (i + j, ((-1)^j u + v)c^{ij})$ is a dihedral automorphic loop. We show that two such loops are isomorphic if and only if the invertible elements coincide, and we calculate the automorphism groups of these loops.

Csörgő showed in [7] that if $Q$ is a finite automorphic loop and $x \in Q$, then $|x|$ divides $|Q|$. This allows us to classify all automorphic loops of order $2p$. There are $p$ such loops up to isomorphism; these are precisely the dihedral automorphic loops corresponding to the $p - 1$ invertible elements of $\mathbb{Z}_p$ and the cyclic group $\mathbb{Z}_{2p}$.

## 2. Preliminaries

The inner mapping group $\mathrm{Inn}(Q)$ has a standard set of generators [2]:

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

Thus automorphic loops can be characterized equationally.

**Proposition 2.1** ([3]). *A loop $Q$ is an automorphic loop if and only if, for all $x$, $y$, $u$, $v \in Q$,*

$$(uv)R_{x,y} = uR_{x,y} \cdot vR_{x,y}, \tag{$A_r$}$$

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

$$(uv)T_x = uT_x \cdot vT_x. \tag{$A_m$}$$

This means that automorphic loops form a variety in the sense of universal algebra. In particular, subloops and factor loops of automorphic loops are automorphic [3, Thm. 2.2].

A loop $Q$ is *power-associative* if for each $x \in Q$, $\langle x \rangle$ is a group. In particular, powers of $x$ are unambiguous, and $x^m x^n = x^{m+n}$ for all $m$, $n \in \mathbb{Z}$.

**Proposition 2.2** ([3, Thm. 2.4]). *Every automorphic loop is power-associative.*

We will use the power-associativity of automorphic loops without explicitly referring to Proposition 2.2.

**Proposition 2.3** ([3, Thm. 2.5]). *Let $Q$ be an automorphic loop. Then the following hold for all $x \in Q$, $j$, $k$, $m$, $n \in \mathbb{Z}$.*

$$L_{x^m}^j L_{x^n}^k = L_{x^n}^k L_{x^m}^j, \tag{2.1}$$

$$R_{x^m}^j L_{x^n}^k = L_{x^n}^k R_{x^m}^j, \tag{2.2}$$

$$R_{x^m}^j R_{x^n}^k = R_{x^n}^k R_{x^m}^j. \tag{2.3}$$

**Corollary 2.4.** *For all $x$ in an automorphic loop $Q$,*

$$L_{x,x^{-1}} = L_{x^{-1},x}, \tag{2.4}$$

$$R_{x,x^{-1}} = R_{x^{-1},x}. \tag{2.5}$$

A loop $Q$ is said to have the *antiautomorphic inverse property* (AAIP) if it has two-sided inverses and satisfies the identity

$$(xy)^{-1} = y^{-1}x^{-1} \tag{AAIP}$$

for all $x$, $y \in Q$. It is also useful to characterize the AAIP in terms of translations and the *inversion mapping* $J : Q \to Q; x \mapsto x^{-1}$ as either of the following:

$$R_x^J = L_{x^{-1}}, \tag{2.6}$$

$$L_x^J = R_{x^{-1}}. \tag{2.7}$$

**Proposition 2.5** ([20, Cor. 6.6]). *Every automorphic loop has the AAIP.*

**Corollary 2.6.** *If $Q$ is an automorphic loop, then $J$ normalizes $\mathrm{Mlt}(Q)$ in $\mathrm{Sym}(Q)$.*

*Proof.* Since $\mathrm{Mlt}(Q)$ is generated by left translations, this follows from (2.6) and (2.7) in view of Proposition 2.5. □

**Lemma 2.7.** *In an automorphic loop $Q$, the following hold for all $x$, $y \in Q$.*

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

$$T_x^{-1} = T_{x^{-1}}. \tag{2.9}$$

*Proof.* We compute

$$R_{x,y} = R_{x,y}^J = R_x^J R_y^J (R_{xy}^{-1})^J = L_{x^{-1}} L_{y^{-1}} L_{(xy)^{-1}}^{-1} = L_{x^{-1}} L_{y^{-1}} L_{y^{-1}x^{-1}}^{-1} = L_{x^{-1},y^{-1}}\,,$$

where we used $R_{x,y} \in \mathrm{Aut}(Q)$ in the first equality, (2.6) in the third, and (AAIP) in the fourth. This establishes (2.8). For (2.9), we have

$$\begin{aligned} T_x T_{x^{-1}} &= R_x L_x^{-1} R_{x^{-1}} L_{x^{-1}}^{-1} = R_x R_{x^{-1}} L_x^{-1} L_{x^{-1}}^{-1} \\ &= R_{x,x^{-1}} L_{x^{-1},x}^{-1} = R_{x,x^{-1}} R_{x,x^{-1}}^{-1} = \mathrm{id}_Q\,, \end{aligned}$$

where we used (2.2) in the second equality, and (2.8) in the fourth. □

To check that a particular loop is automorphic, it is not necessary to verify all of the conditions $(A_r)$, $(A_\ell)$ and $(A_m)$:

**Proposition 2.8** ([20, Thm. 6.7])**.** *Let $Q$ be a loop satisfying $(A_m)$ and $(A_\ell)$. Then $Q$ is automorphic.*

The *left*, *right*, and *middle nuclei* of a loop $Q$ are defined, respectively, by

$$\begin{aligned} N_\lambda(Q) &= \{a \in Q \mid ax \cdot y = a \cdot xy, \quad \forall x,\, y \in Q\}, \\ N_\rho(Q) &= \{a \in Q \mid xy \cdot a = x \cdot ya, \quad \forall x,\, y \in Q\}, \\ N_\mu(Q) &= \{a \in Q \mid xa \cdot y = x \cdot ay, \quad \forall x,\, y \in Q\}, \end{aligned}$$

and the *nucleus* is $N(Q) = N_\lambda(Q) \cap N_\rho(Q) \cap N_\mu(Q)$. Each of these is a subloop.

Recall that a subloop $S \leq Q$ is normal in $Q$, $S \trianglelefteq Q$, if $(S)\varphi = S$ for all $\varphi \in \mathrm{Inn}(Q)$.

**Proposition 2.9.** *Let $Q$ be an automorphic loop. Then*

(i) *$N_\lambda(Q) = N_\rho(Q) \subseteq N_\mu(Q)$, and*
(ii) *each nucleus is normal in $Q$.*

*Proof.* The equality $N_\lambda(Q) = N_\rho(Q)$ is an immediate consequence of the AAIP. Suppose $a \in N_\lambda(Q)$. Then $a^{-1} \in N_\lambda(Q)$ and $(x)T_a = a^{-1}xa$. Now for all $x$, $y \in Q$,

$$(x \cdot ay)T_a = (x)T_a \cdot (ay)T_a = (a^{-1}xa) \cdot ya = a^{-1}(xa \cdot y)a = (xa \cdot y)T_a\,,$$

where we used $(A_m)$ in the first equality, and the equality of the left and right nuclei in the third. Since $T_a$ is a permutation, we have $x \cdot ay = xa \cdot y$ for all $x$, $y \in Q$, that is, $a \in N_\mu(Q)$. This establishes (i). Part (ii) is [3, Thm. 2.2(iii)]. □

For a subset $S$ of a loop $Q$, we define the *commutant of $S$* to be the set

$$C_Q(S) = \{a \in Q \mid ax = xa \quad \text{for all} \quad x \in S\}\,.$$

The *commutant* of $Q$ itself, $C_Q(Q)$, is just denoted by $C(Q)$. (In a group, the commutant of a set is the centralizer of the set and the commutant is the center. However, "center" has a narrower meaning in loop theory, and so we adapt operator theory terminology to the present setting.)

**Proposition 2.10.** *Let $Q$ be an automorphic loop and let $S \subseteq Q$. Then $C_Q(S) \leq Q$. Furthermore, if $S \trianglelefteq Q$, then $C_Q(S) \trianglelefteq Q$. In particular, the commutant $C(Q)$ is a normal subloop of $Q$.*

*Proof.* We have $a \in C_Q(S)$ if and only if $(a)T_x = a$ for all $x \in S$. Thus $C_Q(S)$ is characterized as the intersection of the fixed point sets of all $T_x$, $x \in S$. Since $T_x \in \mathrm{Aut}(Q)$, the fixed point set of $T_x$ is a subloop of $Q$, and $C_Q(S) \leq Q$ follows.

Now suppose $S \trianglelefteq Q$. Fix $a \in C_Q(S)$, $x \in S$, $\varphi \in \mathrm{Inn}(Q)$ and set $y = (x)\varphi^{-1} \in S$. Then

$$x(a)\varphi = (y)\varphi(a)\varphi = (ya)\varphi = (ay)\varphi = (a)\varphi(y)\varphi = (a)\varphi x\,,$$

using $\varphi \in \mathrm{Aut}(Q)$ in the first and fourth equalities and $a \in C_Q(S)$ in the third. Since $x \in S$ was arbitrary, $(a)\varphi \in C_Q(S)$. Thus $C_Q(S) \trianglelefteq Q$. □

We conclude the section with several definitions needed throughout the paper.

A subset $S$ of a loop $Q$ is said to be *characteristic* in $Q$, denoted by $S \operatorname{char} Q$, if for every $\varphi \in \mathrm{Aut}(Q)$, $(S)\varphi = S$. A loop is *characteristically simple* if it has no nontrivial characteristic subloops. A loop is *simple* if it has no nontrivial normal subloops.

A loop $Q$ is *solvable* if it has a subnormal series $1 = Q_0 \leq \cdots \leq Q_n = Q$, $Q_i \trianglelefteq Q_{i+1}$, such that each factor loop $Q_{i+1}/Q_i$ is an abelian group.

The *derived subloop* $Q'$ of a loop $Q$ is the smallest normal subloop of $Q$ such that $Q/Q'$ is an abelian group. The derived subloop can be characterized as the smallest normal subloop containing each *commutator* $[x, y]$, defined by $xy \cdot [y, x] = yx$, and each *associator* $[x, y, z]$, defined by $xy \cdot z = (x \cdot yz)[x, y, z]$. Since automorphisms evidently map commutators to commutators and associators to associators, it follows that $Q' \operatorname{char} Q$.

The *higher derived subloops* are defined in the usual way: $Q^{(2)} = Q'' = (Q')'$, $Q^{(3)} = Q'''$, etc. Note that a loop $Q$ is solvable if and only if $Q^{(n)} = 1$ for some $n > 0$.

A *Bruck loop* is a loop satisfying the *left Bol identity* $(x(yx))z = x(y(xz))$ and the *automorphic inverse property* $(xy)^{-1} = x^{-1}y^{-1}$.

## 3. Cores and twisted subgroups

In an automorphic loop $Q$, we introduce a new binary operation $*$ as follows:

$$x * y = x^{-1}\backslash(y^{-1}x) = (x^{-1}\backslash y^{-1})x \tag{$*$}$$

for all $x$, $y \in Q$. (The second equality follows from (2.2).) We will refer to the magma $(Q, *)$ as the *core* of the loop $Q$, which should not be confused with the core of a subgroup in group theory. A similar notion was introduced by Bruck [2] for Moufang loops (where the operation can be more simply written as $xy^{-1}x$) and also in our previous papers [17, 18] in the commutative case.

As in [14, 17, 18], it is useful to introduce the following permutations for each $x$ in an automorphic loop $Q$:

$$P_x = R_x L_{x^{-1}}^{-1} = L_{x^{-1}}^{-1} R_x, \tag{P}$$

where the second equality follows by Proposition 2.3. Thus the left translation maps of the core $(Q, *)$ are just the maps $JP_x$, $x \in Q$, a fact we will use heavily.

**Proposition 3.1.** *Let $Q$ be an automorphic loop with core $(Q, *)$. Then for all $x$, $y$, $z \in Q$,*

$$(y * z)R_x = yR_x * zR_x, \tag{3.1}$$

$$(y * z)L_x = yL_x * zL_x. \tag{3.2}$$

*Therefore* $\mathrm{Mlt}(Q) \leq \mathrm{Aut}(Q, *)$. *In particular, $P_x \in \mathrm{Aut}(Q, *)$ for all $x \in Q$.*

*Proof.* We start with (2.8), which we write as $R_{y,x} = L_{y^{-1},x^{-1}}$, i.e., $L_{y^{-1}} L_{x^{-1}} L^{-1}_{(yx)^{-1}} = R_y R_x R^{-1}_{yx}$. Rearranging this, we have $L_{x^{-1}} L^{-1}_{(yx)^{-1}} R_{yx} = L^{-1}_{y^{-1}} R_y R_x$ or

$$L_{x^{-1}} P_{yx} = P_y R_x \,. \tag{3.3}$$

Applying both sides of (3.3) to $z^{-1}$ yields $(yx)^{-1}\backslash[(x^{-1}z^{-1}) \cdot yx] = [y^{-1}\backslash(z^{-1}y)]x$. Since $x^{-1}z^{-1} = (zx)^{-1}$ by the AAIP, we have (3.1).

To establish (3.2), observe first that $((1/y)x^{-1})^{-1} = x(1/y)^{-1} = xy$ by AAIP, and so $R_y^{-1} R_{x^{-1}} R_{xy}$ is an inner mapping, hence an automorphism. Thus

$$R_y^{-1} R_{x^{-1}} R_{xy} = (R_y^{-1} R_{x^{-1}} R_{xy})^J = (R_y^{-1})^J R^J_{x^{-1}} R^J_{xy} = L^{-1}_{y^{-1}} L_x L_{(xy)^{-1}} \,,$$

using (2.6) and (2.7). Rearranging, we have $R_{x^{-1}} R_{xy} L^{-1}_{(xy)^{-1}} = R_y L^{-1}_{y^{-1}} L_x$ or

$$R_{x^{-1}} P_{xy} = P_y L_x \,. \tag{3.4}$$

Applying both sides of (3.4) to $z^{-1}$ yields $(xy)^{-1}\backslash[(z^{-1}x^{-1}) \cdot xy] = x[y^{-1}\backslash(z^{-1}y)]$. Since $z^{-1}x^{-1} = (xz)^{-1}$ by the AAIP, we are finished. □

**Lemma 3.2.** *For all $x$ in an automorphic loop $Q$,*

$$P_x^J = P_x^{-1} = P_{x^{-1}} \,. \tag{3.5}$$

*Thus in the core $(Q, *)$, the following holds for all $x$, $y \in Q$:*

$$(x * y)^{-1} = x^{-1} * y^{-1} \,. \tag{3.6}$$

*Proof.* We have $P_x^J = R_x^J (L^{-1}_{x^{-1}})^J = L_{x^{-1}} R_x^{-1} = P_x^{-1}$, using (2.6) and (2.7). Also,

$$P_x P_{x^{-1}} = R_x L^{-1}_{x^{-1}} R_{x^{-1}} L_x^{-1} = R_x L_x^{-1} R_{x^{-1}} L^{-1}_{x^{-1}} = T_x T_{x^{-1}} = \mathrm{id}_Q \,,$$

using (2.2) and (2.1) in the second equality and (2.9) in the fourth. This establishes (3.5). Then (3.6) follows, since $(x * y)^{-1} = yJP_xJ = yP_x^J = (y^{-1})JP_{x^{-1}} = x^{-1} * y^{-1}$. □

**Theorem 3.3.** *Let $Q$ be an automorphic loop with core $(Q, *)$. Then $(Q, *)$ is an involutive quandle; that is, the following properties hold:*

(i) *$x * x = x$ for all $x \in Q$,*
(ii) *$x * (x * y) = y$ for all $x$, $y \in Q$,*
(iii) *$x * (y * z) = (x * y) * (x * z)$ for all $x$, $y$, $z \in Q$.*

*Proof.* Part (i) is clear from the definition of $*$. For (ii), $x * (x * y) = yJP_xJP_x = yP_x^J P_x = y$ by (3.5). For (iii),

$$x * (y * z) = (y * z)JP_x = (y^{-1} * z^{-1})P_x = (y^{-1})P_x * (z^{-1})P_x = (x * y) * (x * z) \,,$$

using (3.6) and Proposition 3.1. □

Recall that a subset $A$ of a group $G$ is said to be a *twisted subgroup* of $G$ if (i) $1 \in A$, (ii) $a \in A$ implies $a^{-1} \in A$, and (iii) $a, b \in A$ implies $aba \in A$.

In an automorphic loop $Q$, let $P_Q = \{P_x \,|\, x \in Q\}$.

**Proposition 3.4.** *Let $Q$ be an automorphic loop. Then $P_Q$ is a twisted subgroup of* $\mathrm{Mlt}(Q)$. *In particular,*

$$P_x P_y P_x = P_{yP_x} \tag{3.7}$$

*for all $x$, $y \in Q$.*

*Proof.* Clearly $\mathrm{id}_Q = P_1 \in P_Q$. For $x \in Q$, $P_x^{-1} \in P_Q$ by (3.5). Since $JP_x \in \mathrm{Aut}(Q,*)$ by Theorem 3.3(iii), we have $zJP_yJP_x = (y*z)JP_x = yJP_x * zJP_x = zJP_xJP_{yJP_x}$ for all $x$, $y$, $z \in Q$. Thus $P_y^J P_x = P_x^J P_{(y^{-1})P_x}$. By (3.5), we deduce $P_xP_{y^{-1}}P_x = P_{(y^{-1})P_x}$. Replacing $y$ with $y^{-1}$, we have (3.7). □

**Corollary 3.5.** *Let $Q$ be an automorphic loop. Then for all $x \in Q$ and $n \in \mathbb{Z}$,*

$$P_x^n = P_{x^n}\,. \tag{3.8}$$

*Proof.* Since $(x^n)P_x = x^{n+2}$, the desired result follows for $n \geq 0$ by an easy induction using (3.7). For $n < 0$, apply (3.5). □

Although we have no application for the following result, we mention it for the sake of completeness:

**Proposition 3.6.** *Let $Q$ be an automorphic loop. Then $\langle P_Q\rangle \trianglelefteq \mathrm{Mlt}(Q)$.*

*Proof.* By (3.3), we have for each $x, y \in Q$, $R_x^{-1}P_yR_x = R_x^{-1}L_{x^{-1}}P_{yx} = P_x^{-1}P_{yx} \in \langle P_Q\rangle$. By (3.4), we have for each $x, y \in Q$, $L_x^{-1}P_yL_x = L_x^{-1}R_{x^{-1}}P_{xy} = P_{x^{-1}}P_{xy} \in \langle P_Q\rangle$. Since $\mathrm{Mlt}(Q)$ is generated by all $R_x$, $L_x$, $x \in Q$, we have the desired result. □

## 4. Uniquely 2-divisible automorphic loops

A loop $Q$ is said to be *uniquely 2-divisible* if the squaring map $x \mapsto x^2$ is a permutation of $Q$.

**Lemma 4.1.** *Let $Q$ be a uniquely 2-divisible automorphic loop. Then $Q \to P_Q; x \mapsto P_x$ is a bijection.*

*Proof.* To see that the map is one-to-one, suppose $P_x = P_y$. Applying both sides to 1, we obtain $x^2 = y^2$. By unique 2-divisibility, $x = y$. □

It is well known that a uniquely 2-divisible twisted subgroup $T$ of a group $G$ can be turned into a Bruck loop $(T, \bullet)$ by setting

$$a \bullet b = (ab^2a)^{1/2}. \tag{$\bullet$}$$

See [11, Lem. 4.5], for instance.

In a uniquely 2-divisible automorphic loop $Q$, the set $P_Q$ is a uniquely 2-divisible twisted subgroup of $\mathrm{Mlt}(Q)$ by Proposition 3.4 and Corollary 3.5, noticing that $P_x^{1/2} = P_{x^{1/2}}$ for all $x \in Q$. Thus we can define

$$P_x \bullet P_y = [P_xP_y^2P_x]^{1/2} = P_{(y^2)P_x}^{1/2} = P_{[(y^2)P_x]^{1/2}},$$

making $(P_Q, \bullet)$ into a Bruck loop.

Upon defining $(Q, \circ)$ on $Q$ by

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

we see that the bijection $(Q, \circ) \to (P_Q, \bullet)$; $x \mapsto P_x$ is an isomorphism of magmas. Thus $(Q, \circ)$ is a Bruck loop, the *Bruck loop associated with the uniquely 2-divisible automorphic loop $Q$*.

We have established most of the following:

**Proposition 4.2.** *Let $Q$ be a uniquely 2-divisible automorphic loop. Then $(Q, \circ)$ defined by ($\circ$) is a Bruck loop. Powers in $(Q, \circ)$ coincide with powers in $Q$. Any subloop of $Q$ which is closed under square roots is a subloop of $(Q, \circ)$.*

*Proof.* We already showed that $(Q, \circ)$ is a Bruck loop. Powers of $x$ in $(Q, \circ)$ correspond to powers of $P_x$ in $(P_Q, \bullet)$. But these coincide with powers of $P_x$ in $\mathrm{Mlt}(Q)$ [11, Lem. 4.5]. By Corollary 3.5, we conclude that powers in $(Q, \circ)$ coincide with powers in $Q$. In Bruck loops, the left and right divisions can be expressed in terms of the multiplication and inversion: $x \backslash_\circ y = x^{-1} \circ y$ and $x /_\circ y = y^{-1} \circ ((y \circ x) \circ y^{-1})$. Thus the claim about subloops follows directly from $(\circ)$. □

Note that $x \circ y = [(x^{-1} \backslash y^2)x]^{1/2} = [x^{-1} \backslash (y^2 x)]^{1/2}$ by Proposition 2.3.

**Proposition 4.3.** *Let $Q$ be a uniquely 2-divisible automorphic loop. Then the core $(Q, *)$ is a quasigroup.*

*Proof.* This follows immediately from the unique 2-divisibility, the fact that $(Q, \circ)$ is a loop, and the observation $x * y = (x \circ y^{-1/2})^2$. □

The *left multiplication group* $\mathrm{Mlt}_\lambda(Q)$ of a loop $Q$ is the group $\langle L_x \mid x \in Q \rangle \leq \mathrm{Mlt}(Q)$.

**Lemma 4.4.** *Let $Q$ be a uniquely 2-divisible automorphic loop with associated Bruck loop $(Q, \circ)$. Then $\mathrm{Mlt}_\lambda(Q, \circ)$ is conjugate in $\mathrm{Sym}(Q)$ to $\langle P_Q \rangle$.*

*Proof.* Let $\sigma : Q \to Q; x \mapsto x^2$ denote the squaring permutation. For each $x \in Q$, the left translation $y \mapsto x \circ y$ is just $\sigma P_x \sigma^{-1}$. This establishes the desired result. □

We will need the following easy observation later.

**Lemma 4.5.** *Let $Q$ be a uniquely 2-divisible automorphic loop with associated Bruck loop $(Q, \circ)$. Then $\mathrm{Aut}(Q) \leq \mathrm{Aut}(Q, \circ)$. In particular, every inner mapping of $Q$ acts as an automorphism of $(Q, \circ)$.*

Next, we prove the Lagrange and Cauchy Theorems for automorphic loops of odd order. First, we must show that for finite automorphic loops, the notions of unique 2-divisibility and having odd order coincide. In fact, this is true more generally for finite power-associative loops.

**Lemma 4.6.** *Let $Q$ be a finite loop with two-sided inverses.*

(i) *If $Q$ is uniquely 2-divisible, then $Q$ has odd order.*
(ii) *If $Q$ has odd order and the AAIP, then $Q$ has no elements of order 2. If $Q$ is also power-associative, then $Q$ is uniquely 2-divisible.*

*Proof.* Suppose $Q$ is uniquely 2-divisible. Then the inversion mapping $J$ fixes only the identity element. Since $J$ has order 2, the set of nonidentity elements of $Q$ must have even order, and so $Q$ has odd order. This proves (i).

Now assume $Q$ has odd order and the AAIP, and suppose $c \in Q$ satisfies $c^2 = 1$. By the AAIP, if $xy = c$, then $c = c^{-1} = (xy)^{-1} = y^{-1}x^{-1}$. Thus the set $K = \{(x, y) \mid xy = c\}$ is invariant under the mapping $\phi : Q^2 \to Q^2; (x, y) \mapsto (y^{-1}, x^{-1})$. Since $\phi$ is involutive and $|K|$ is odd, $\phi$ has a fixed point $(x, y) \in K$. This point satisfies $x^{-1} = y$, so that $1 = xx^{-1} = c$. This establishes the first part of (ii), and the remaining assertion is clear. □

**Corollary 4.7.** *A finite automorphic loop is uniquely 2-divisible if and only if it has odd order.*

**Corollary 4.8.** *Let $Q$ be a finite automorphic loop of even order. Then $Q$ contains an element of order 2.*

*Proof.* Otherwise, every element of $Q$ would have odd order, so that $Q$ would be uniquely 2-divisible, and hence have odd order. □

**Lemma 4.9.** *Let $Q$ be an automorphic loop of odd order with associated Bruck loop $(Q, \circ)$. If $S$ is a subloop of $Q$, then $S$ is a subloop of $(Q, \circ)$.*

*Proof.* In this case, the square root of any element is a positive integer power of that element, and so subloops are closed under taking square roots. Then Proposition 4.2 applies. □

**Theorem 4.10** (Lagrange Theorem)**.** *Let $Q$ be an automorphic loop of odd order. If $S \leq Q$, then $|S|$ divides $|Q|$.*

*Proof.* By Lemma 4.9, $S$ is a subloop of the associated Bruck loop $(Q, \circ)$. The result follows from [13, Cor. 4]. □

Note that Theorem 4.10, sometimes called the weak Lagrange property, implies what is known as the strong Lagrange property for automorphic loops of odd order: if $T \leq S \leq Q$, then $|T|$ divides $|S|$. This is because subloops of automorphic loops of odd order are themselves automorphic loops of odd order.

**Theorem 4.11** (Cauchy Theorem)**.** *Let $Q$ be an automorphic loop of odd order. If a prime $p$ divides $|Q|$, then $Q$ contains an element of order $p$.*

*Proof.* By [13, Cor. 1, p. 394], the associated Bruck loop $(Q, \circ)$ contains an element of order $p$ and thus so does $Q$ by Proposition 4.2. □

**Corollary 4.12.** *Every automorphic loop of prime order is a group.*

*Proof.* This is trivial for $p = 2$, while for $p$ odd, it follows from Theorem 4.11. □

## 5. A correspondence with Lie rings

Following Wright [28], if $(A, +, \cdot)$ is an algebra (over some field), define $(A, \diamond)$ by $x \diamond y = x + y - xy$. By [28, Prop. 8], $(A, \diamond)$ is a loop if and only if the mappings $y \mapsto y - yx$, $y \mapsto y - xy$ are bijections of $A$. We will now specialize this construction to Lie rings and establish its partial inverse.

Recall that a *Lie ring* $(Q, +, [\cdot, \cdot])$ is an abelian group $(Q, +)$ such that the bracket $[\cdot, \cdot]$ is biadditive, satisfies the Jacobi identity $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$, and is alternating, that is, $[x, x] = 0$. Consequently, Lie rings are skew-symmetric, $[x, y] = -[y, x]$.

As usual, for $x \in Q$ define $\mathrm{ad}(x) : Q \to Q$; $y \mapsto [y, x]$. Thanks to skew-symmetry, the mappings from Wright's construction take on the form

$$r_x = \mathrm{id}_Q - \mathrm{ad}(x);\ y \mapsto y - [y, x],$$
$$\ell_x = \mathrm{id}_Q + \mathrm{ad}(x);\ y \mapsto y + [y, x].$$

Note that all $r_x$, $\ell_x$ are homomorphisms of $(Q, +)$.

In this context, Wright's construction can be stated as follows:

**Lemma 5.1.** *Let $(Q, +, [\cdot, \cdot])$ be a Lie ring. Then $(Q, \diamond)$ defined by*

$$(\diamond) \qquad x \diamond y = x + y - [x, y]$$

*is a loop (with neutral element 0) if and only if $(Q, +, [\cdot, \cdot])$ satisfies $(W_1)$, that is, if and only if the mappings $r_x$, $\ell_x$ are invertible for every $x \in Q$.*

*For $x \in Q$ let $R_x^\diamond$, $L_x^\diamond$ be the right and left translations by $x$ in the groupoid $(Q, \diamond)$. Then*

$$y \diamond x = yR_x^\diamond = x + yr_x,$$
$$x \diamond y = yL_x^\diamond = x + y\ell_x.$$

*If $(Q, \diamond)$ is a loop, then also*

$$y(R_x^\diamond)^{-1} = (y - x)r_x^{-1},$$
$$y(L_x^\diamond)^{-1} = (y - x)\ell_x^{-1},$$
$$R_y^\diamond R_z^\diamond (R_{y\diamond z}^\diamond)^{-1} = r_y r_z r_{y\diamond z}^{-1},$$
$$L_y^\diamond L_z^\diamond (L_{z\diamond y}^\diamond)^{-1} = \ell_y \ell_z \ell_{z\diamond y}^{-1},$$
$$R_y^\diamond (L_y^\diamond)^{-1} = r_y \ell_y^{-1}.$$

*Proof.* The first part of the statement is a special case of Wright's result, and the formulae for the translations $R_x^\diamond$, $L_x^\diamond$ follow from $(\diamond)$ and skew-symmetry. For the rest of the proof suppose that $(Q, \diamond)$ is a loop. We immediately get the formulae for $(R_x^\diamond)^{-1}$ and $(L_x^\diamond)^{-1}$. Finally,

$$\begin{aligned} xR_y^\diamond R_z^\diamond (R_{y\diamond z}^\diamond)^{-1} &= (z + (y + xr_y)r_z - (y \diamond z))r_{y\diamond z}^{-1} \\ &= (z + yr_z + xr_y r_z - (z + yr_z))r_{y\diamond z}^{-1} \\ &= xr_y r_z r_{y\diamond z}^{-1}, xL_y^\diamond L_z^\diamond (L_{z\diamond y}^\diamond)^{-1} = (z + (y + x\ell_y)\ell_z - (z \diamond y))\ell_{z\diamond y}^{-1} \\ &= (z + y\ell_z + x\ell_y\ell_z - (z + y\ell_z))\ell_{z\diamond y}^{-1} = x\ell_y\ell_z\ell_{z\diamond y}^{-1}, \end{aligned}$$

and

$$xR_y^\diamond (L_y^\diamond)^{-1} = ((y + xr_y) - y)\ell_y^{-1} = xr_y\ell_y^{-1}.$$

□

The Lie ring construction sometimes yields automorphic loops:

**Proposition 5.2.** *Let $(Q, +, [\cdot, \cdot])$ be a Lie ring satisfying $(W_1)$ and $(W_2)$. Then $(Q, \diamond)$ defined by $(\diamond)$ is an automorphic loop, and the commutant and nuclei of $(Q, \diamond)$ are given by*

$$C(Q, \diamond) = \{a \in Q \mid 2[a, x] = 0,\ \forall x \in Q\},$$
$$N_\lambda(Q, \diamond) = \{a \in Q \mid [[a, x], y] = 0,\ \forall x,\ y \in Q\},$$
$$N_\mu(Q, \diamond) = \{a \in Q \mid [[x, y], a] = 0,\ \forall x,\ y \in Q\}.$$

*In particular, $(Q, \diamond)$ is a group if and only if $[[x, y], z] = 0$ for all $x$, $y$, $z \in Q$.*

*Proof.* By Lemma 5.1, $(Q, \diamond)$ is a loop. For all $x$, $y$, $z \in Q$, we have

$$\begin{aligned} xr_z \diamond yr_z &= x - [x, z] + y - [y, z] - [x - [x, z], y - [y, z]] \\ &= x + y - [x, y] - [x + y, z] + [x, [y, z]] + [[x, z], y] - [[x, z], [y, z]] \\ &= x + y - [x, y] - [x + y, z] + [[x, y], z] \\ &= (x \diamond y)r_z\,, \end{aligned}$$

where we have used both the Jacobi identity and the condition $(W_2)$ in the third equality. Thus for each $z \in Q$ we have $r_z \in \mathrm{Aut}(Q, \diamond)$. Similarly, $\ell_z \in \mathrm{Aut}(Q, \diamond)$. By Lemma 5.1, the standard generators $R_y^\diamond R_z^\diamond (R_{y\diamond z}^\diamond)^{-1}$, $L_y^\diamond L_z^\diamond (L_{z\diamond y}^\diamond)^{-1}$ and $R_y^\diamond (L_y^\diamond)^{-1}$

of $\mathrm{Inn}(Q,\diamond)$ are elements of $\langle r_x, \ell_x \mid x \in Q\rangle \leq \mathrm{Aut}(Q,\diamond)$, and hence $(Q,\diamond)$ is an automorphic loop.

The characterization of the commutant is clear from $(\diamond)$. For the nuclei, we compute

$$\big((x \diamond y) \diamond z\big) - \big(x \diamond (y \diamond z)\big) = [[x,y],z] - [x,[y,z]] = [[x,z],y]\,,$$

using the Jacobi identity. Thus a triple $x$, $y$, $z$ associates in $(Q,\diamond)$ if and only if $[[x,z],y] = 0$. All remaining claims easily follow. □

**Corollary 5.3.** *Let $Q$ be a Lie ring satisfying $(W_1)$ and $(W_2)$, and let $(Q,\diamond)$ be the corresponding automorphic loop.*

(i) *If $Q$ has characteristic 2, then $(Q,\diamond)$ is commutative.*
(ii) *If the abelian group $(Q,+)$ is uniquely 2-divisible, then $C(Q,\diamond) = Z(Q,\diamond)$ is equal to the center of the Lie ring $Q$.*

For the rest of this section we will be concerned with the question of whether it is possible to invert the construction of Proposition 5.2 to obtain a Lie ring satisfying $(W_1)$ and $(W_2)$ from an automorphic loop. We identify suitable subclasses of Lie rings and automorphic loops when this is indeed the case.

For the rest of this section we will deal with uniquely 2-divisible automorphic loops $Q$ for which the associated Bruck loop $(Q,\circ)$ is a group, hence an abelian group. For $x$ in such a loop $Q$, define the inner mapping

$$(\phi) \qquad \phi_x = R_x P_{x^{1/2}}^{-1}.$$

We will make heavy use of the fact that $\phi_x \in \mathrm{Aut}(Q)$, often without explicit reference.

**Lemma 5.4.** *Let $Q$ be a uniquely 2-divisible automorphic loop for which the associated Bruck loop $(Q,\circ)$ is an abelian group. For all $x$, $y \in Q$, the following identities hold:*

$$xy = (x)\phi_y \circ y, \tag{5.1}$$

$$x \circ (y^{-1})\phi_x = y^{-1} \circ (x)\phi_y. \tag{5.2}$$

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

$$x^2y^2 = (x^2)R_{y^2}P_y^{-1}P_y = (x^2)\phi_{y^2}P_y = [((x)\phi_{y^2})^2]P_y = [(x)\phi_{y^2} \circ y]^2\,.$$

Since $(Q,\circ)$ is an abelian group and powers in $(Q,\cdot)$, $(Q,\circ)$ coincide, we have $x^2y^2 = ((x)\phi_{y^2})^2 \circ y^2 = (x^2)\phi_{y^2} \circ y^2$. Replacing $x$ with $x^{1/2}$ and $y$ with $y^{1/2}$, we obtain (5.1).

Now using AAIP, we have

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

Replacing $x$ with $x^{-1}$, we obtain (5.2). □

**Lemma 5.5.** *Let $Q$ be a uniquely 2-divisible automorphic loop for which the associated Bruck loop $(Q,\circ)$ is an abelian group. Then $P_Q = \langle P_Q\rangle$ is an abelian group isomorphic to $(Q,\circ)$. In particular, for all $x$, $y \in Q$,*

$$P_xP_y = P_{x\circ y}\,. \tag{5.3}$$

*Proof.* Since $(Q,\circ)$ is an abelian group, $(Q,\circ) \cong \mathrm{Mlt}_\lambda(Q,\circ) \cong \langle P_Q\rangle$ by Lemma 4.4. For (5.3), we have $P_{x\circ y} = P_x \bullet P_y = (P_xP_y^2P_x)^{1/2} = (P_x^2P_y^2)^{1/2} = P_xP_y$, since $\langle P_Q\rangle$ is an abelian group. □

**Lemma 5.6.** *Let $Q$ be a uniquely 2-divisible automorphic loop for which the associated Bruck loop $(Q,\circ)$ is an abelian group. Then $\langle \phi_x \mid x\in Q\rangle = \mathrm{Inn}(Q)$.*

*Proof.* One inclusion is obvious. We have

(5.4)
$$R_{x,y} = R_xR_yR_{xy}^{-1} = \phi_xP_{x^{1/2}}\phi_yP_{y^{1/2}}P_{(xy)^{1/2}}^{-1}\phi_{xy}^{-1} = \phi_x\phi_yP_{(x^{1/2})\phi_y}P_{y^{1/2}}P_{(xy)^{1/2}}^{-1}\phi_{xy}^{-1},$$

since $\phi_y\in\mathrm{Aut}(Q)$. Now by (5.3), $P_{(x^{1/2})\phi_y}P_{y^{1/2}} = P_{(x^{1/2})\phi_y\circ y^{1/2}}$. By the fact that $(Q,\circ)$ is an abelian group and (5.1), $(x^{1/2})\phi_y\circ y^{1/2} = [(x)\phi_y\circ y]^{1/2} = (xy)^{1/2}$. Thus (5.4) reduces to $R_{x,y} = \phi_x\phi_y\phi_{xy}^{-1}$. By (2.8), $L_{x,y} = R_{x^{-1},y^{-1}} = \phi_{x^{-1}}\phi_{y^{-1}}\phi_{x^{-1}y^{-1}}^{-1}$. Finally,

$$T_x = R_xL_x^{-1} = \phi_xP_{x^{1/2}}L_x^{-1} = \phi_xP_{x^{1/2}}P_{x^{-1}}R_{x^{-1}}^{-1} = \phi_xP_{x^{-1/2}}R_{x^{-1}}^{-1} = \phi_x\phi_{x^{-1}}^{-1},$$

where we used (5.3) and $x^{1/2}\circ x^{-1} = x^{-1/2}$ in the fourth equality. It follows that $\mathrm{Inn}(Q)\le\langle\phi_x\mid x\in Q\rangle$. □

A Lie ring $(Q,+,[\cdot,\cdot])$ is said to be *uniquely 2-divisible* if the abelian group $(Q,+)$ is uniquely 2-divisible.

**Theorem 5.7** (Partial correspondence between Lie rings and automorphic loops)**.** *Suppose that $(Q,+,[\cdot,\cdot])$ is a uniquely 2-divisible Lie ring satisfying $(W_1)$ and $(W_2)$. Then $(Q,\diamond)$ defined by*

$$x\diamond y = x+y-[x,y]$$

*is a 2-divisible automorphic loop whose associated Bruck loop $(Q,\circ)$ is an abelian group; in fact, $(Q,\circ)=(Q,+)$.*

*Conversely, suppose that $(Q,\cdot)$ is a uniquely 2-divisible automorphic loop whose associated Bruck loop $(Q,\circ)$ is an abelian group. Then $(Q,\circ,[\cdot,\cdot])$ defined by*

$$([\cdot,\cdot]) \qquad [x,y] = x\circ y\circ(xy)^{-1}$$

*is a uniquely 2-divisible Lie ring satisfying $(W_1)$ and $(W_2)$.*

*Furthermore, the two constructions are inverses of each other. Subrings (resp. ideals) of the Lie ring are subloops (resp. normal subloops) of the corresponding automorphic loop, and subloops (resp. normal subloops) closed under square roots are subrings (resp. ideals) of the corresponding Lie ring.*

*Proof.* Suppose that $(Q,+,[\cdot,\cdot])$ is a uniquely 2-divisible Lie ring satisfying $(W_1)$ and $(W_2)$. By Proposition 5.2, $(Q,\diamond)$ is an automorphic loop. Note that $x\diamond x = 2x$, $x^{-1} = -x$ and $x^{1/2} = \frac{1}{2}x$. The multiplication in the Bruck loop $(Q,\circ)$ associated with $(Q,\diamond)$ therefore has the form $x\circ y = ((2y)(L_{-x}^{\diamond})^{-1}R_x^{\diamond})\frac{1}{2} = ((2y)R_x^{\diamond}(L_{-x}^{\diamond})^{-1})\frac{1}{2}$, where the second equality follows by Proposition 2.3. Showing $x\circ y = x+y$ is therefore equivalent to proving $(2y)\diamond x = (2y)R_x^{\diamond} = (2x+2y)L_{-x}^{\diamond} = (-x)\diamond(2x+2y)$. But $(2y)\diamond x = 2y+x-[2y,x] = (-x)+(2x+2y)-[-x,2x+2y] = (-x)\diamond(2x+2y)$.

Conversely, suppose that $(Q,\cdot)$ is a uniquely 2-divisible automorphic loop whose associated Bruck loop $(Q,\circ)$ is an abelian group. By (5.1), we have $[x,y] = x\circ y\circ(xy)^{-1} = x\circ y\circ((x)\phi_y\circ y)^{-1} = x\circ y\circ(x^{-1})\phi_y\circ y^{-1} = x\circ(x^{-1})\phi_y$. Since $(x^{-1})\phi_x = x^{-1}$, we have $[x,x]=1$. Next,

$$\begin{aligned}[x,y]\circ[y,x] &= x\circ(x^{-1})\phi_y\circ y\circ(y^{-1})\phi_x = x\circ(y^{-1})\phi_x\circ y\circ(x^{-1})\phi_y\\ &= (x)\phi_y\circ y^{-1}\circ y\circ(x^{-1})\phi_y = 1,\end{aligned}$$

where we have used (5.2) in the third equality and $\phi_y \in \mathrm{Aut}(Q) \leq \mathrm{Aut}(Q, \circ)$ in the last equality. For biadditivity, we compute

$$[x \circ y, z] = x \circ y \circ [(x \circ y)^{-1}]\phi_z = x \circ (x^{-1})\phi_z \circ y \circ (y^{-1})\phi_z = [x, z] \circ [y, z],$$
$$[x, y \circ z] = [y \circ z, x]^{-1} = ([y, x] \circ [z, x])^{-1} = [y, x]^{-1} \circ [z, x]^{-1} = [x, y] \circ [x, z].$$

So far we have shown that $(Q, \circ, [\cdot, \cdot])$ is an alternating, biadditive (nonassociative) ring with underlying abelian group $(Q, \circ)$. In what follows the symbols $+$ and $-$ will refer to sums and differences of endomorphisms of $(Q, \circ)$. Rearranging the definition of $[\cdot, \cdot]$ and using the skew-symmetry, we have $xy = x \circ y \circ [x, y]^{-1} = y \circ (x)(\mathrm{id}_Q - \mathrm{ad}(y))$. Comparing this with (5.1), we see that $\mathrm{id}_Q - \mathrm{ad}(x) = \phi_x$ and also $\mathrm{id}_Q + \mathrm{ad}(x) = \phi_{x^{-1}}$. In particular, property $(W_1)$ holds.

Now using biadditivity, we have

$$[(x)(\mathrm{id}_Q + \mathrm{ad}(z)), (y)(\mathrm{id}_Q + \mathrm{ad}(z))] = [x, y] \circ [x, [y, z]] \circ [[x, z], y] \circ [[x, z], [y, z]],$$

and also

$$[x, y](\mathrm{id}_Q + \mathrm{ad}(z)) = [x, y] \circ [[x, y], z].$$

Since $\mathrm{id}_Q + \mathrm{ad}(x) = \phi_x \in \mathrm{Aut}(Q) \leq \mathrm{Aut}(Q, [\cdot, \cdot])$, the results of these two calculations are equal. Canceling common terms and rearranging using skew-symmetry, we obtain

$$[[x, y], z] \circ [[y, z], x] \circ [[z, x], y] = [[x, z], [y, z]] \tag{5.5}$$

for all $x$, $y$, $z \in Q$. Since the left side of (5.5) is invariant under cyclic permutations of $x$, $y$, $z$, so is the right side, and so we have

$$[[x, z], [y, z]] = [[y, x], [z, x]] \tag{5.6}$$

for all $x$, $y$, $z \in Q$. Replace $x$ in this last identity with $x \circ u$ and use biadditivity to get

$$[[x, z], [y, z]] \circ [[u, z], [y, z]] = [[y, x], [z, x]] \circ [[y, u], [z, x]] \circ [[y, x], [z, u]] \circ [[y, u], [z, u]].$$

Canceling terms on both sides using (5.6), we obtain $1 = [[y, u], [z, x]] \circ [[y, x], [z, u]]$ for all $x$, $y$, $z$, $u \in Q$. Taking $u = y$, we get $1 = [[y, x], [z, y]]$, which is equivalent to $(W_2)$. It follows that the right side of (5.5) is equal to 1, and so the Jacobi identity holds. Therefore, $(Q, \circ, [\cdot, \cdot])$ is a Lie ring satisfying $(W_1)$ and $(W_2)$.

Let us now show that the two constructions are inverse to each other. Suppose that the constructions yield $(Q, \cdot) \mapsto (Q, \circ, [\cdot, \cdot]) \mapsto (Q, \diamond)$. Then $x \diamond y = x \circ y \circ [x, y]^{-1}$, and since $(Q, \circ)$ is an abelian group and $x \circ y \circ (xy)^{-1} = [x, y]$, we conclude that $x \diamond y = xy$. In the other direction, let $(Q, +, [\cdot, \cdot]) \mapsto (Q, \diamond) \mapsto (Q, \circ, \lceil \cdot, \cdot \rceil)$, where $(Q, \circ)$ is the Bruck loop associated with $(Q, \diamond)$. We have already shown that $(Q, \circ) = (Q, +)$. Then $\lceil x, y \rceil = x \circ y \circ (x \diamond y)^{-1} = x + y - (x + y - [x, y]) = [x, y]$.

Finally, we show the correspondence of substructures. Suppose that $(Q, \cdot)$ corresponds to $(Q, +, [\cdot, \cdot])$. Lemma 5.1 shows that the three loop operations of $(Q, \cdot)$ (in fact, of $(Q, \diamond)$, but $(Q, \diamond) = (Q, \cdot)$ here) can be expressed in terms of $+$ and $[\cdot, \cdot]$.

If $S$ is a subring of $(Q, +, [\cdot, \cdot])$, then since $S$ is closed under $+$ and $[\cdot, \cdot]$, it is a subloop of $(Q, \cdot)$. If $S$ is an ideal of $(Q, +, [\cdot, \cdot])$, then it is invariant under the mappings $\mathrm{id}_Q - \mathrm{ad}(x) = \phi_x$ for all $x \in Q$, and hence $S$ is invariant under $\mathrm{Inn}(Q, \cdot)$ by Lemma 5.6.

If $S$ is a subloop of $(Q, \cdot)$ closed under square roots, then by Proposition 4.2 $S$ is a subgroup of $(Q, \circ)$. Therefore $S$ is a subring of $(Q, +, [\cdot, \cdot])$ by definition of the bracket.

Finally, if $S$ is a normal subloop of $(Q,\cdot)$, then $S$ is invariant under all mappings $\mathrm{id}_Q - \mathrm{ad}(x) = \phi_x$. But then $(S)\mathrm{ad}(x) \subseteq S$ for all $x \in Q$, and so $S$ is an ideal of $(Q,+,[\cdot,\cdot])$. □

We conclude with the observation that in the uniquely 2-divisible case the condition $(W_2)$ already implies that $(Q,+,[\cdot,\cdot])$ is solvable of derived length at most 2.

**Lemma 5.8.** *Let $(Q,+,[\cdot,\cdot])$ be a uniquely 2-divisible Lie ring. Then $Q$ satisfies $(W_2)$ if and only if $[[Q,Q],[Q,Q]] = 0$.*

*Proof.* Clearly, if $[[Q,Q],[Q,Q]] = 0$, then $(W_2)$ follows. For the converse, suppose that $[[x_1,x_2],[x_3,x_4]] = 0$ for all $x_i \in Q$, $i = 1,\dots,4$. Replacing $x_2$ with $x_2 + x_4$ and then using $(W_2)$ itself to cancel terms, we obtain $[[x_1,x_2],[x_3,x_4]] + [[x_1,x_4],[x_3,x_2]] = 0$ or by skew-symmetry,

$$[[x_1,x_2],[x_3,x_4]] = [[x_1,x_4],[x_2,x_3]] \tag{5.7}$$

for all $x_i \in Q$, $i = 1,\dots,4$. Set $v = [[x_1,x_2],[x_3,x_4]]$. Under the natural action of the symmetric group $S_4$ on functions from $Q^4$ to $Q$, skew-symmetry and (5.7) imply that $v^\sigma = (-1)^\sigma v$ for all $\sigma \in S_4$. Hence $v = v^{(13)(24)} = [[x_3,x_4],[x_1,x_2]] = -[[x_1,x_2],[x_3,x_4]] = -v$. Thus $2v = 0$, and so $v = 0$ by unique 2-divisibility. □

## 6. Nilpotency and solvability

In this section we prove the Odd Order Theorem for automorphic loops together with two other corollaries of Theorem 5.7. We start with automorphic loops of prime power order.

Let $p$ be a prime. By Corollary 4.12, an automorphic loop of order $p$ is isomorphic to $\mathbb{Z}_p$. The following result was first obtained by Csörgő [6], using her signature method of connected transversals. We can now give a short proof based on Theorem 5.7. A proof that is both short and elementary remains elusive.

**Theorem 6.1** (Csörgő)**.** *Let $p$ be a prime. Every automorphic loop of order $p^2$ is a group.*

*Proof.* Let $Q$ be an automorphic loop of order $p^2$. Every loop of order 4 is associative [25], so assume $p > 2$. Bruck loops of order $p^2$ are groups [4]. If $(Q,\circ)$ is cyclic, then so is $Q$, so assume $(Q,\circ)$ is elementary abelian. Theorem 5.7 and Lemma 5.8 give an associated solvable Lie ring $(Q,\circ,[\cdot,\cdot])$ of derived length at most 2. Since $(Q,\circ)$ is an elementary abelian, $(Q,\circ,[\cdot,\cdot])$ is a 2-dimensional Lie algebra over $GF(p)$. Over any field, there are, up to isomorphism, only two 2-dimensional Lie algebras, one abelian and the other nonabelian [16]. The nonabelian Lie algebra of dimension 2 has a basis $\{x,y\}$ such that $[x,y] = y$. But then $y(\mathrm{id} + \mathrm{ad}(x)) = 0$ so that condition $(W_1)$ is not satisfied. Thus $(Q,\circ,[\cdot,\cdot])$ must be an abelian Lie algebra, that is, $[x,y] = 0$ for all $x, y \in Q$. Then $xy = x \circ y$; that is, $Q$ is an abelian group. □

Commutative automorphic loops of order $p^k$ are centrally nilpotent when $p$ is an odd prime [5, 19]. Commutative automorphic loops of order $p^3$ were classified up to isomorphism in [8]. There are additional nonassociative noncommutative automorphic loops of order $p^3$, $p$ and odd prime. A class of such loops with trivial nuclei was obtained in [19]. In particular, when $p$ is an odd prime, automorphic loops of order $p^3$ need not be centrally nilpotent. In the following example we present the construction of [19] in a new way, using the corresponding Lie algebras.

**Example 6.2.** Let $F$ be a field and fix $A \in GL(2, F)$. On $Q = F \times F^2$, define an operation $[\cdot, \cdot]$ by

$$[(a, x), (b, y)] = (0, (ay - bx)A)$$

for all $a$, $b \in F$, $x$, $y \in F^2$. (Note that we think of elements of $F^2$ as row vectors so that $A$ acts on the right.) Then it is straightforward to verify that $(Q, +, [\cdot, \cdot])$ is a Lie algebra satisfying $(W_2)$. Let $r_x = \mathrm{id}_Q - \mathrm{ad}(x)$, $\ell_x = \mathrm{id}_Q + \mathrm{ad}(x)$ be as before. In block matrix form, we have

$$(a, x)r_{(b,y)} = (a, x + (bx - ay)A) = (a, x) \begin{pmatrix} 1 & -yA \\ 0 & I + bA \end{pmatrix}$$

and

$$(b, y)\ell_{(a,x)} = (b, y + (bx - ay)A) = (b, y) \begin{pmatrix} 1 & xA \\ 0 & I - aA \end{pmatrix},$$

where $I$ is the $2 \times 2$ identity matrix. Thus condition $(W_1)$ will hold precisely when $\det(I + \mu A) \neq 0$ for all $\mu \in F$, that is, when the characteristic polynomial of $A$ has no roots in $F$. (See [19] for an interpretation of this in terms of anisotropic planes.) Assume this property now holds for $A$.

We show that the left/right nucleus of the corresponding loop $(Q, \diamond)$ is trivial. By Proposition 5.2, $N_\lambda(Q, \diamond)$ consists of all elements $(a, x)$ such that

$$[[(a, x), (b, y)], (c, z)] = (0, c(ay - bx)A) = (0, 0)$$

for all $b$, $c \in F$, $y$, $z \in F^2$. Thus $c(ay - bx)A = 0$. Since $A \in GL(2, F)$ and taking $c \neq 0$, we have $ay = bx$ for all $b \in F$, $y \in F^2$. Taking $b \neq 0$, $y = 0$ implies $x = 0$, while taking $b = 0$, $y \neq 0$ implies $a = 0$. Thus $N_\lambda(Q, \diamond)$ is trivial.

Consider the particular case $F = GF(p)$. If $p = 2$, then by Corollary 5.3, we obtain a commutative automorphic loop $(Q, \diamond)$ of exponent 2 and order 8. There is precisely one such loop with trivial center, first constructed in [18]. As discussed in [19], if $p = 3$, then this construction gives two isomorphism classes of (noncommutative) automorphic loops depending on the choice of $A$, while if $p = 5$, there are three isomorphism classes. For $p > 5$, it is conjectured that there are precisely three isomorphism classes [19, Conj. 6.5].

Returning to general automorphic loops of order $p^3$, $p$ odd prime, there is much that is still unknown, but we can at least say that for $p = 3$, such automorphic loops are necessarily given by the construction of Proposition 5.2:

**Lemma 6.3.** *Let $Q$ be an automorphic loop of order 27 and exponent 3. Then $Q$ is constructed from a Lie algebra satisfying $(W_1)$ and $(W_2)$ by the construction $(\diamond)$.*

*Proof.* Every Bruck loop of exponent 3 is a commutative Moufang loop [26]. Moufang loops of order $3^n$ for $n \leq 3$ are associative. Thus the associated Bruck loop $(Q, \circ)$ is an elementary abelian 3-group. By Theorem 5.7, we have an associated solvable Lie ring $(Q, \circ, [\cdot, \cdot])$ satisfying $(W_1)$, $(W_2)$. Since $(Q, \circ)$ is elementary abelian, $(Q, \circ, [\cdot, \cdot])$ is a Lie algebra over $GF(3)$. By Theorem 5.7, $(Q, \cdot)$ is equal to the loop $(Q, \diamond)$ obtained from $(Q, \circ, [\cdot, \cdot])$ by $(\diamond)$. □

Lemma 6.3 cannot be easily extended to Bruck loops of order $p^3$ and exponent $p$ for $p > 3$ because there are nonassociative Bruck loops of such orders.

We now start working toward the Odd Order Theorem.

If $Q$ is a loop and $S \leq Q$, the *relative multiplication group of* $S$, denoted by $\mathrm{Mlt}(Q;S)$, is the subgroup of $\mathrm{Mlt}(Q)$ generated by all $R_x$, $L_x$, $x \in S$. The *relative inner mapping group of* $S$ is $\mathrm{Inn}(Q;S) = (\mathrm{Mlt}(Q;S))_1 = \mathrm{Mlt}(Q;S) \cap \mathrm{Inn}(Q)$.

**Lemma 6.4.** *Let $Q$ be a finite automorphic loop of odd order. A subloop $S$ of the associated Bruck loop $(Q,\circ)$ is a subloop of $Q$ if and only if $Sh = S$ for every $h \in \mathrm{Inn}(Q;S)$.*

*Proof.* The "only if" direction is trivial, so assume the hypothesis of the converse assertion. Fix $u, v \in S$. Since powers agree in $(Q,\circ)$ and $Q$, we have $u^{-1}, v^{-1} \in S$. Set $w = v^{1/2}$ and note that $v \in S$ as well. By Lemma 4.5, $\mathrm{Aut}(Q,\cdot) \leq \mathrm{Aut}(Q,\circ)$. Thus $S$ also contains

$$\begin{aligned}(u \circ w)^2 T_u &= (uT_u \circ wT_u)^2 = (u \circ wT_u)^2 = (u^{-1} \backslash [wT_u]^2)u \\ &= vT_u L_{u^{-1}}^{-1} R_u = vR_u^2 L_u^{-1} L_{u^{-1}}^{-1},\end{aligned}$$

using (2.2). Since $L_{u^{-1}} L_u \in \mathrm{Inn}(Q)$, $S$ also contains $vR_u^2 = (u \circ w)^2 T_u L_{u^{-1}} L_u$. By induction, $vR_u^{2k} \in S$ for all integers $k$. Now let $2n+1$ be the order of $u$. Then $R_u^{2n+1} \in \mathrm{Inn}(Q)$, and so $S$ contains $vR_u^{2n+1} R_u^{-2n} = vu$, and also $vR_u^{2n+1} R_u^{2(-n-1)} = v/u$. Thus $S$ is closed under multiplication and right division. By the AAIP, $S$ is also closed under left division, and hence is a subloop. □

**Lemma 6.5.** *Let $Q$ be a uniquely 2-divisible automorphic loop, and let $(Q,\circ)$ be the associated Bruck loop. Then every characteristic subloop of $(Q,\circ)$ is a normal subloop of $Q$.*

*Proof.* If $S$ is a characteristic subloop of $(Q,\circ)$, then by Lemma 4.5, $S$ is invariant under $\mathrm{Inn}(Q)$. By Lemma 6.4, $S$ is a subloop of $Q$. □

**Theorem 6.6** (Odd Order Theorem)**.** *Every automorphic loop of odd order is solvable.*

*Proof.* Let $Q$ be a minimal counterexample. If $1 < S \lhd Q$, then by minimality, both $S$ and $Q/S$ are solvable automorphic loops of odd order. This contradicts the nonsolvability of $Q$. Therefore $Q$ is simple.

Let $(Q,\circ)$ be the associated Bruck loop and let $D$ denote the derived subloop of $(Q,\circ)$. By [14, Thm. 14(b)], $(Q,\circ)$ is solvable and so $D$ is a proper subloop. Since $D\,\mathrm{char}(Q,\circ)$, it follows from Lemma 6.5 that $D \trianglelefteq Q$. Since $Q$ is simple, $D = \{1\}$. Therefore $(Q,\circ)$ is an abelian group.

Now let $p$ be a prime divisor of $|Q|$ and let $M_p = \{x \in Q \mid x^p = 1\}$. Then $M_p\,\mathrm{char}(Q,\circ)$, and so by Lemma 6.5 again, $M_p \trianglelefteq Q$. By Theorem 4.11, $M_p$ is nontrivial, and so since $Q$ is simple, $M_p = Q$. Thus $Q$ has exponent $p$, $(Q,\circ)$ has exponent $p$ by Proposition 4.2, and $(Q,\circ)$ is an elementary abelian $p$-group.

By Theorem 5.7, $(Q,\circ,[\cdot,\cdot])$ defined by $([\cdot,\cdot])$ is a Lie ring satisfying $(W_1)$ and $(W_2)$. By Lemma 5.8, $(Q,\circ,[\cdot,\cdot])$ is solvable. Since $(Q,\circ)$ is an elementary abelian $p$-group, we may view $(Q,\circ,[\cdot,\cdot])$ as a finite-dimensional Lie algebra over $GF(p)$. Since $Q$ is simple as a loop, Theorem 5.7 also implies that $(Q,\circ,[\cdot,\cdot])$ is either simple as a Lie algebra or else is abelian. The former case contradicts the solvability of $(Q,\circ,[\cdot,\cdot])$, and so $(Q,\circ,[\cdot,\cdot])$ is abelian. But then $xy = x \circ y \circ [x,y] = x \circ y$, so that $Q$ is an abelian group, a contradiction with nonsolvability of $Q$. □

We remark that the proof of [14, Thm. 14(b)] depends on the Feit-Thompson Odd Order Theorem for groups, and hence so does our proof of Theorem 6.6.

## 7. Finite simple automorphic loops

The main open problem in the theory of automorphic loops is the existence or nonexistence of a nonassociative finite simple automorphic loop; *cf.*, Problem 10.1. By Theorem 6.6 and by the main results of [15], such a loop would be noncommutative and of even order, though not a 2-loop.

Simple loops can be studied via primitive permutation groups thanks to this classic theorem of Albert [1]:

**Proposition 7.1.** *A loop $Q$ is simple if and only if* $\mathrm{Mlt}(Q)$ *is primitive.*

**Lemma 7.2.** *Let $Q$ be a simple nonassociative automorphic loop with inversion map $J$. If $J \neq \mathrm{id}_Q$, then $C_{\mathrm{Mlt}(Q)}(J) = \mathrm{Inn}(Q)$.*

*Proof.* Since $Q$ is automorphic, $J$ commutes with every inner mapping. Therefore $\mathrm{Inn}(Q) \leq C_{\mathrm{Mlt}(Q)}(J)$. Since $\mathrm{Mlt}(Q)$ is primitive by Proposition 7.1, $\mathrm{Inn}(Q)$ is a maximal subgroup of $\mathrm{Mlt}(Q)$. Since $J \neq \mathrm{id}_Q$, there is $x \in Q$ such that $x \neq x^{-1}$, and so $xJL_x = 1 \neq x^{-2} = xL_xJ$. Hence $C_{Mlt(Q)}(J) \neq \mathrm{Mlt}Q$, and so the desired equality holds. □

Recall that the *socle* $\mathrm{Soc}(G)$ of a group $G$ is the subgroup generated by the minimal normal subgroups of $G$. By the O'Nan-Scott Theorem [9, Thm. 4.1A], the analysis of a finite primitive group $G$ divides into two cases depending on whether or not $\mathrm{Soc}(G)$ is regular.

**Proposition 7.3.** *Let $Q$ be a finite simple nonassociative automorphic loop. Then the socle* $\mathrm{Soc}(\mathrm{Mlt}(Q))$ *is not regular.*

*Proof.* Suppose $S = \mathrm{Soc}(\mathrm{Mlt}(Q))$ is regular. Recall that $J$ normalizes $\mathrm{Mlt}(Q)$ in $\mathrm{Sym}(Q)$ by Corollary 2.6. Thus since $S$ is characteristic in $\mathrm{Mlt}(Q)$, $S$ is normalized by $J$. By Theorem 6.6, $|S| = |Q|$ is even. Thus $J$ fixes a nonidentity element $s \in S$. If $J \neq \mathrm{id}_Q$, then by Lemma 7.2, $s \in \mathrm{Inn}(Q)$. But then $(1)s = 1$, which contradicts the regularity of $S$. Therefore $J = \mathrm{id}_Q$ and so $Q$ has exponent 2. By [17, Thm. 6.2], $Q$ has order a power of 2 and then by [15, Thm. 3], $Q$ is solvable, a contradiction. □

By the O'Nan-Scott Theorem, it follows that $\mathrm{Mlt}(Q)$ is of almost simple type, of diagonal type or of product type [9].

Although the classification of finite simple automorphic loops remains open, results from group theory about characteristic subgroups hold analogously for characteristic subloops of automorphic loops with essentially the same proofs (*cf.* the closing remarks of [15]). Part (ii) of the following result is [3, Thm. 2.2(ii)].

**Theorem 7.4.** *Let $Q$ be an automorphic loop.*

(i) *If $T \operatorname{char} S \trianglelefteq Q$, then $T \trianglelefteq Q$.*
(ii) *Every characteristic subloop of $Q$ is normal.*
(iii) *If $Q$ is finite and characteristically simple, then $Q$ is a direct product of isomorphic simple loops.*

*Proof.* Every inner mapping leaves $S$ invariant, hence acts as an automorphism of $S$. Since $T$ is characteristic in $S$, $T\varphi = T$ for all $\varphi \in \mathrm{Inn}(Q)$. This establishes (i), and (ii) follows from (i) by taking $S = Q$. Now suppose $Q$ is finite and characteristically simple, and let $S = S_1$ be a minimal normal subloop. Consider the orbit

$\{S_1, \ldots, S_m\}$ of $S$ under $\mathrm{Aut}(Q)$. Each $S_i$, being the image of a minimal normal subloop of $Q$ under an automorphism, is also a minimal normal subloop of $Q$. Since each $S_i \cap S_j$ is normal in $Q$, it follows from minimality that the subloops $S_i$ intersect pairwise trivially. Thus $S_1 \cdots S_m$ is a direct product [2]. Since automorphisms map the direct factors of $S_1 \cdots S_m$ to each other, the direct product is characteristic in $Q$. Thus $Q = S_1 \cdots S_m$ because $Q$ is characteristically simple. Since $S$ is both a minimal normal subloop and a direct factor of $Q$, $S$ must be simple. This establishes (iii). □

**Corollary 7.5.** *A minimal normal subloop of a finite automorphic loop is a direct product of isomorphic simple loops.*

*Proof.* If $S$ is a minimal normal subloop of $Q$, then by Theorem 7.4(i), $S$ is characteristically simple, and we are done by Theorem 7.4(iii). □

**Proposition 7.6.** *Let $Q$ be an automorphic loop.*

(i) *$Q^{(n)} \trianglelefteq Q$ for each $n > 0$.*
(ii) *If $Q$ is solvable, then the* derived series *$Q \trianglerighteq Q' \trianglerighteq Q'' \trianglerighteq \cdots \trianglerighteq Q^{(n)} = 1$ is a normal series, that is, $Q^{(k)} \trianglelefteq Q$ for all $k > 0$.*

*Proof.* Each $Q^{(k)}$ is characteristic in $Q^{(k-1)}$ for all $k \geq 1$. By Theorem 7.4(i), each $Q^{(n)} \trianglelefteq Q$. This proves (i), and (ii) follows from (i). □

## 8. Split middle nuclear extensions

In this brief section we will examine automorphic loops which are split extensions by their middle nuclei. The following proposition shows that this notion can be defined in either of the usual group theoretic ways.

**Proposition 8.1.** *Let $Q$ be a loop with normal middle nucleus $N_\mu = N_\mu(Q)$. The following conditions are equivalent.*

(i) *The natural homomorphism $\eta : Q \to Q/N_\mu$ splits; that is, there is a homomorphism $\sigma : Q/N_\mu \to Q$ such that $\sigma\eta = \mathrm{id}_{Q/N_\mu}$.*
(ii) *There exists a subloop $S$ of $Q$ such that $Q = SN_\mu$ and $S \cap N_\mu = 1$.*

*Proof.* Assume (i) holds. Let $S = \sigma(Q/N_\mu)$, which is a subloop of $Q$ since $\sigma$ is a homomorphism. Clearly $S \cap N_\mu = 1$. For $x \in Q$, let $s = (x)\eta\sigma = (xN_\mu)\sigma$ and let $a = s\backslash x$. Then $(a)\eta = N_\mu$, that is, $a \in \ker(\eta) = N_\mu$. Therefore $Q = SN_\mu$ and (ii) holds.

Assume (ii) holds. Suppose $sa = tb$ for $s, t \in S$ and $a, b \in N_\mu$. Then $s = tb \cdot a^{-1} = t \cdot ba^{-1}$ since $a, b \in N_\mu$. Hence $t\backslash s = ba^{-1} \in S \cap N_\mu = 1$, and so $t = s$ and $b = a$. Thus each $x \in Q$ has a unique factorization $x = sa$ for some $s \in S$, $a \in N_\mu$. In particular, the subloop $S$ is a complete set of left coset representatives of $N_\mu$. Therefore setting $(sN_\mu)\sigma = s$ for each $s \in S$ yields a well-defined map $\sigma : Q/N_\mu \to Q$ with $(sN_\mu)\eta\sigma = sN_\mu$. Finally $\sigma$ is a homomorphism by the definition of coset multiplication. □

We will say that an automorphic loop $Q$ is a *split middle nuclear extension* (of $S$ by $N_\mu$) if either, and hence both, of the conditions of Proposition 8.1 holds. In automorphic loops, the multiplication in a split middle nuclear extension has a very specific form, as follows.

**Proposition 8.2.** *Let $Q$ be an automorphic loop. For all $a$, $b \in N_\mu(Q)$ and all $x$, $y \in Q$,*

$$xa \cdot yb = xy \cdot ((a)T_y \cdot b)L_{y,x}\,. \tag{8.1}$$

*Proof.* First we prove

$$a \cdot yb = ay \cdot b\,. \tag{8.2}$$

Since $b \in N_\mu = N_\mu(Q)$, we have $T_b = R_b L_{b^{-1}}$. Thus we compute

$$\begin{aligned} ay \cdot b = b \cdot (ay)T_b = b[(a)T_b \cdot (y)T_b] = b[b^{-1}ab \cdot b^{-1}yb] \\ = b[b^{-1}a \cdot yb] = (b \cdot b^{-1}a) \cdot yb = a \cdot yb, \end{aligned}$$

where we have used $T_b \in \mathrm{Aut}(Q)$ in the second equality, $b, b^{-1} \in N_\mu$ in the fourth equality and $b^{-1}a \in N_\mu$ in the fifth equality. This establishes (8.2).

For (8.1), we compute

$$xa \cdot yb = x(a \cdot yb) \overset{(8.2)}{=} x(ay \cdot b) = x \cdot (y \cdot (a)T_y)b = x \cdot y((a)T_y \cdot b) = xy \cdot ((a)T_y \cdot b)L_{y,x}\,,$$

where we have used $(a)T_y \in N_\mu$ (since $N_\mu \trianglelefteq Q$ by Proposition 2.9) in the fourth equality. □

**Corollary 8.3.** *Let $Q$ be an automorphic loop which is a split middle nuclear extension $Q = SN_\mu$. Then for all $s$, $t \in S$, $a$, $b \in N_\mu$,*

$$sa \cdot tb = st \cdot ((a)T_t \cdot b)L_{t,s}\,, \tag{8.3}$$

*where the right hand side is the unique factorization of the left side into an element $st \in S$ and an element $((a)T_t \cdot b)L_{t,s} \in N_\mu$.*

Just as split extensions of groups (internal semidirect products) lead naturally to external semidirect products, so do split middle nuclear extensions of automorphic loops lead to an "external" construction of automorphic loops. The input data are a loop $S$, a group $N$, a mapping $\phi : S \to \mathrm{Aut}(N)$ satisfying $(1)\phi = 1$ and a mapping $\alpha : S \times S \to \mathrm{Aut}(N)$ satisfying $(1, s)\alpha = (s, 1)\alpha = 1$ for all $s \in S$. On $Q := S \times N$, we define operations by

$$\begin{aligned} (s, a) \cdot (t, b) &= (st, (a^{(t)\phi}b)^{(t,s)\alpha})\,, \\ (s, a)\backslash(t, b) &= (s\backslash t, (a^{-1})^{(s\backslash t)\phi}b^{((s\backslash t,s)\alpha)^{-1}})\,, \\ (s, a)/(t, b) &= (s/t, (a^{((t,s/t)\alpha)^{-1}}b^{-1})^{((t)\phi)^{-1}})\,. \end{aligned}$$

Then it is easy to show $(Q, \cdot, \backslash, /)$ is a loop with neutral element $(1, 1)$. To get an automorphic loop, it is necessary that $S$ be automorphic, and there are various conditions which must be satisfied by $\phi$ and $\alpha$. It is straightforward to find these conditions by simply calculating inner mappings in $Q$ and assuming them to be automorphisms. However, the calculations and the conditions themselves are both lengthy and unenlightening in their full generality. Since we are only going to examine a special case in detail in the next section, we omit the general construction.

## 9. Dihedral automorphic loops

We begin with a construction of automorphic loops motivated by Corollary 8.3.

**Proposition 9.1.** *Let $(A,+)$ be an abelian group and fix $\alpha \in \mathrm{Aut}(A)$. Let $\mathrm{Dih}(A,\alpha)$ be defined on $\mathbb{Z}_2 \times A$ by*

$$(i,u)\cdot(j,v) = (i+j, ((-1)^j u + v)\alpha^{ij}). \tag{9.1}$$

*Then $(\mathrm{Dih}(A,\alpha),\cdot)$ is an automorphic loop. If $\alpha \neq \mathrm{id}_A$, then $N_\mu = \{0\}\times A \cong A$.*

*Proof.* Throughout the proof, the exponent of $\alpha$ in (9.1) is calculated in $\mathbb{Z}_2$. Clearly $(0,0)$ is the neutral element. Setting

$$\begin{aligned}(i,u)\backslash(j,v) &= (i+j, v\alpha^{-i(j+i)} - (-1)^{i+j}u),\\ (i,u)/(j,v) &= (i+j, (-1)^j(u\alpha^{-(i+j)j} - v),\end{aligned}$$

it is straightforward to show that $\backslash$ and $/$ satisfy the properties of divisions in a loop.

The generalized conjugation $T_{(i,u)}$ is given by

$$(j,v)T_{(i,u)} = \left(j, (-1)^i v + (1-(-1)^j)u\right),$$

as can be readily checked. Note that this is independent of $\alpha$. We check that this is an automorphism. First,

$$\begin{aligned}[(j,v)\cdot(k,w)]T_{(i,u)} &= (j+k, ((-1)^k v + w)\alpha^{jk})T_{(i,u)}\\ &= (j+k, (-1)^i((-1)^k v + w)\alpha^{jk} + (1-(-1)^{j+k})u)\\ &= (j+k, (-1)^{i+k}v\alpha^{jk} + (-1)^i w\alpha^{jk} + (1-(-1)^{j+k})u).\end{aligned}$$

On the other hand,

$$\begin{aligned}&(j,v)T_{(i,u)}\cdot(k,w)T_{(i,u)}\\ &\quad= (j,(-1)^i v + (1-(-1)^j)u)\cdot(k,(-1)^i w + (1-(-1)^k)u)\\ &\quad= (j+k, [(-1)^k((-1)^i v + (1-(-1)^j)u) + (-1)^i w + (1-(-1)^k)u]\alpha^{jk})\\ &\quad= (j+k, (-1)^{i+k}v\alpha^{jk} + (-1)^i w\alpha^{jk} + h),\end{aligned}$$

where

$$h = [(-1)^k(1-(-1)^j) + (1-(-1)^k)]u\alpha^{jk} = (1-(-1)^{j+k})u\alpha^{jk}.$$

Checking all four possibilities, we see that $(1-(-1)^{j+k})u\alpha^{jk} = (1-(-1)^{j+k})u$ for $j,k\in\mathbb{Z}_2$. Thus $T_{(i,u)}$ is an automorphism.

Next, we check that the left inner mappings $L_{(j,v),(i,u)}$ are automorphisms. A lengthy calculation gives

$$(k,w)L_{(j,v),(i,u)} = \left(k, [(-1)^{j+k}u(\alpha^{-jk} - \mathrm{id}_A) + w]\alpha^{ij}\right).$$

Note that this is independent of $v$. We have

$$\begin{aligned}&(k,w)L_{(j,v),(i,u)}\cdot(\ell,x)L_{(j,v),(i,u)}\\ &\quad= (k, [(-1)^{j+k}u(\alpha^{-jk}-\mathrm{id}_A)+w]\alpha^{ij})\cdot(\ell, [(-1)^{j+\ell}u(\alpha^{-j\ell}-\mathrm{id}_A)+x]\alpha^{ij})\\ &\quad= (k+\ell, \{(-1)^\ell[(-1)^{j+k}u(\alpha^{-jk}-\mathrm{id}_A)+w]\\ &\qquad\qquad + (-1)^{j+\ell}u(\alpha^{-j\ell}-\mathrm{id}_A)+x\}\alpha^{ij}\alpha^{k\ell})\\ &\quad= (k+\ell, [(-1)^\ell w + x + q]\alpha^{ij}\alpha^{k\ell}),\end{aligned}$$

where

$$\begin{aligned} q &= (-1)^\ell u[(-1)^{j+k}(\alpha^{-jk} - \mathrm{id}_A) + (-1)^j(\alpha^{-j\ell} - \mathrm{id}_A)] \\ &= (-1)^{j+k+\ell} u(\alpha^{-jk} - \mathrm{id}_A + (-1)^k(\alpha^{-j\ell} - \mathrm{id}_A)) \\ &= (-1)^{j+k+\ell} u(\alpha^{-j(k+\ell)} - \mathrm{id}_A). \end{aligned}$$

The last equality follows by checking all possible values of $j$, $k$, $\ell \in \mathbb{Z}_2$. On the other hand, we compute

$$\begin{aligned} &[(k,w)\cdot(\ell,x)]L_{(j,v),(i,u)} \\ &\quad = (k+\ell, [(-1)^\ell w + x]\alpha^{k\ell}) L_{(j,v),(i,u)} \\ &\quad = (k+\ell, \{(-1)^{j+k+\ell} u(\alpha^{-j(k+\ell)} - \mathrm{id}_A) + [(-1)^\ell w + x]\alpha^{k\ell}\}\alpha^{ij}) \\ &\quad = (k+\ell, \{(-1)^{j+k+\ell} u(\alpha^{-j(k+\ell)} - \mathrm{id}_A)\alpha^{-k\ell} + (-1)^\ell w + x\}\alpha^{k\ell}\alpha^{ij}). \end{aligned}$$

Now observe that $u(\alpha^{-j(k+\ell)} - \mathrm{id}_A)\alpha^{-k\ell} = u(\alpha^{-j(k+\ell)} - \mathrm{id}_A)$ for all $j$, $k$, $\ell \in \mathbb{Z}_2$ just by checking all possibilities. Thus we see that $L_{(j,v),(i,u)}$ is an automorphism.

Applying Proposition 2.8, we have shown that $\mathrm{Dih}(A,\alpha)$ is an automorphic loop. It remains to characterize the middle nucleus when $\alpha \neq \mathrm{id}_A$. We have that $(j,v) \in N_m$ if and only if $(k,w) = (k,w)L_{(j,v),(i,u)}$ for all $i$, $k \in \mathbb{Z}_2$, $u$, $w \in A$. Thus matching second components, we require

$$[(-1)^{j+k} u(\alpha^{-jk} - \mathrm{id}_A) + w]\alpha^{ij} = w \tag{9.2}$$

for all $i$, $k \in \mathbb{Z}_2$, $u$, $w \in A$. Taking $u = 0$, $i = 1$, we must have $w\alpha^j = w$ for all $w \in A$. Thus $\alpha^j = \mathrm{id}_A$. Since $\alpha \neq \mathrm{id}_A$, we must have $j = 0$. On the other hand, since (9.2) is independent of $v$, it is clear that $(0,v) \in N_\mu$. This completes the proof. □

We call the loops $\mathrm{Dih}(A,\alpha)$ *generalized dihedral automorphic loops*. $\mathrm{Dih}(A,\mathrm{id}_A)$ is the usual generalized dihedral group determined by the abelian group $A$. If $A = \mathbb{Z}$, then $\mathrm{Aut}(A) = \mathbb{Z}^* = \{\pm 1\}$. In this case we write $D_\infty(c) = \mathrm{Dih}(\mathbb{Z}, c)$ where $c = \pm 1$ and refer to these loops as *infinite dihedral automorphic loops*. If $A = \mathbb{Z}_n$, then $\mathrm{Aut}(A) = \mathbb{Z}_n^*$, the group of integers in $\{1,\ldots,n-1\}$ coprime to $m$. We write $D_{2n}(c) = \mathrm{Dih}(\mathbb{Z}_n, c)$ where $c \in \mathbb{Z}_n^*$ and refer to these loops simply as *dihedral automorphic loops*.

In $D_\infty(c)$ or $D_{2n}(c)$, the multiplication specializes as follows:

$$(i,j)\cdot(k,\ell) = (i+k, c^{ik}((-1)^k j + \ell)), \tag{9.3}$$

where $c \in \{\pm 1\}$ in the former case and $c \in \mathbb{Z}_n^*$ in the latter case.

We now show that different values of the parameter $c$ give nonisomorphic dihedral automorphic loops, and we calculate their automorphism groups.

**Lemma 9.2.** *Let $Q = D_{2n}(c)$. Then*

(i) $(0,1)^m = (0,m)$ *for every* $m \in \mathbb{Z}$, *and* $\mathbb{Z}_n \cong 0 \times \mathbb{Z}_n \leq Q$,
(ii) $|(1,x)| = 2$ *for every* $x \in \mathbb{Z}_n$,
(iii) $(1,0)\cdot(0,y) = (1,y)$ *for every* $y \in \mathbb{Z}_n$, *and* $Q = \langle (0,1), (1,0)\rangle$.

*Proof.* (i) Since automorphic loops are power-associative, the power $(0,1)^m$ is well defined for every $m \in \mathbb{Z}$. The claim holds for $m = 0$, since $(0,0)$ is the neutral element of $Q$. Suppose the claim holds for some $m \geq 0$. Then $(0,1)^{m+1} = (0,1)^m \cdot (0,1) = (0,m)\cdot(0,1) = (0,m+1)$. Since $(0,-m)\cdot(0,m) = (0,0)$, it follows that $(0,1)^{-m} = (0,-m)$. The rest is clear.

(ii) For any $x \in \mathbb{Z}_n$ we have $(1,x)\cdot(1,x) = (0, c(-x+x)) = (0,0)$.

(iii) The formula $(1,0)\cdot(0,y) = (1,y)$ follows immediately from (9.3). Then $Q = \langle (0,1),(1,0)\rangle$ follows from (i). □

By Lemma 9.2, a loop homomorphism $f : D_{2n}(c) \to Q$ is determined by its values $(0,1)f$, $(1,0)f$. If $n > 2$, then $0 \times \mathbb{Z}_n$ is the unique subloop of $D_{2n}(c)$ isomorphic to $\mathbb{Z}_n$, by Lemma 9.2(iii). Hence, if $f : D_{2n}(c) \to D_{2n}(d)$ is an isomorphism, it follows that $(0,1)f = (0,\alpha)$ for some $\alpha \in \mathbb{Z}_n^*$, and $(1,0)f = (1,\beta)$ for some $\beta \in \mathbb{Z}_n$. Using Lemma 9.2 again, we then have

$$(0,x)f = ((0,1)^x)f = ((0,1)f)^x = (0,\alpha)^x = (0,x\alpha),$$
$$(1,x)f = ((1,0)\cdot(0,x))f = (1,0)f\cdot(0,x)f = (1,\beta)\cdot(0,x\alpha) = (1,\beta+x\alpha)$$

for every $x \in \mathbb{Z}_n$.

Given any $\alpha \in \mathbb{Z}_n^*$, $\beta \in \mathbb{Z}_n$, let us denote the mapping $f : D_{2n}(c) \to D_{2n}(d)$ satisfying $(0,x)f = (0,x\alpha)$, $(1,x)f = (1,\beta+x\alpha)$ for all $x \in \mathbb{Z}_n$ by $f_{\alpha,\beta}$. (Note that the definition of $f_{\alpha,\beta}$ does not require knowledge of $c$, $d$, so we will consider $f_{\alpha,\beta}$ to be a mapping from $D_{2n}(c)$ to $D_{2n}(d)$ for any $c$, $d \in \mathbb{Z}_n^*$.)

**Lemma 9.3.** *Let $c$, $d \in \mathbb{Z}_n^*$, $\alpha \in Z_n^*$ and $\beta \in \mathbb{Z}_n$. Then $f = f_{\alpha,\beta} : D_{2n}(c) \to D_{2n}(d)$ is a bijection that satisfies $((0,x)\cdot(0,y))f = (0,x)f\cdot(0,y)f$, $((0,x)\cdot(1,y))f = (0,x)f\cdot(1,y)f$ and $((1,x)\cdot(0,y))f = (1,x)f\cdot(0,y)f$ for every $x$, $y \in \mathbb{Z}_n$. Moreover, $f$ is an isomorphism if and only if $c = d$.*

*Proof.* Since $\alpha \in \mathbb{Z}_n^*$, it is clear from the definition of $f = f_{\alpha,\beta}$ that it is a bijection $D_{2n}(c) \to D_{2n}(d)$. For $x$, $y \in \mathbb{Z}_n$ we have $((0,x)\cdot(0,y))f = (0,x+y)f = (0,(x+y)\alpha) = (0,x\alpha)\cdot(0,y\alpha) = (0,x)f\cdot(0,y)f$, $((0,x)\cdot(1,y))f = (1,-x+y)f = (1,\beta+(-x+y)\alpha) = (0,x\alpha)\cdot(1,\beta+y\alpha) = (0,x)f\cdot(1,y)f$, and $((1,x)\cdot(0,y))f = (1,x+y)f = (1,\beta+(x+y)\alpha) = (1,\beta+x\alpha)\cdot(0,y\alpha) = (1,x)f\cdot(0,y)f$. Finally, we have $((1,x)\cdot(1,y))f = (0,c(-x+y))f = (0,c(-x+y)\alpha)$, while $(1,x)f\cdot(1,y)f = (1,\beta+x\alpha)\cdot(1,\beta+y\alpha) = (0,d(-(\beta+x\alpha)+\beta+y\alpha)) = (0,d(-x+y)\alpha)$, so $f$ is an isomorphism if and only if $c = d$. □

**Corollary 9.4.** *For an integer $n \geq 2$, the loops $D_{2n}(c)$, $c \in \mathbb{Z}_n^*$, are pairwise nonisomorphic.*

**Proposition 9.5.** *Let $c \in \mathbb{Z}_n^*$ and $Q = D_{2n}(c)$. Then* $\mathrm{Aut}(Q)$ *is isomorphic to the holomorph* $\mathrm{Aut}(\mathbb{Z}_n) \rtimes \mathbb{Z}_n = \mathbb{Z}_n^* \rtimes \mathbb{Z}_n$ *with multiplication $(\alpha,\beta)(\gamma,\delta) = (\alpha\gamma, \beta+\alpha\delta)$.*

*Proof.* By the discussion preceding Lemma 9.3, every automorphism of $Q$ is of the form $f_{\alpha,\beta}$ for some $\alpha \in \mathbb{Z}_n^*$, $\beta \in \mathbb{Z}_n$. By Lemma 9.3, every such mapping $f_{\alpha,\beta}$ is an automorphism of $Q$. Now, if $\gamma \in \mathbb{Z}_n^*$, $\delta \in \mathbb{Z}_n$ and $x \in \mathbb{Z}_n$, we have $(0,x)f_{\gamma,\delta}f_{\alpha,\beta} = (0,x\gamma)f_{\alpha,\beta} = (0,x\gamma\alpha) = (0,x\alpha\gamma) = (0,x)f_{\alpha\gamma,\beta+\alpha\delta}$ and $(1,x)f_{\gamma,\delta}f_{\alpha,\beta} = (1,\delta+x\gamma)f_{\alpha,\beta} = (1,\beta+(\delta+x\gamma)\alpha) = (1,\beta+\alpha\delta+x\alpha\gamma) = (1,x)f_{\alpha\gamma,\beta+\alpha\delta}$. □

Results analogous to 9.2–9.5 hold for the infinite dihedral automorphic loops $D_\infty(c)$, with every occurrence of $\mathbb{Z}_n$ replaced with $\mathbb{Z}$, and $2n$ replaced with $\infty$.

Commutative automorphic loops with middle nuclei of index 2 were studied in detail in [18]. In the next result we examine the noncommutative case under the assumption that the middle nucleus is cyclic.

**Proposition 9.6.** *Let $Q$ be a noncommutative automorphic loop with cyclic middle nucleus $N_\mu(Q) = \langle b \rangle$, and suppose that $Q$ is a split middle nuclear extension $Q = \langle a \rangle \langle b \rangle$ where $a^2 = 1$. If $Q$ is infinite, then $Q \cong D_\infty(c)$ for some $c \in \{\pm 1\}$. If $Q$ is finite, then $Q \cong D_{2n}(c)$ for some $n \in \mathbb{N}$ and some $c \in \mathbb{Z}_n^*$.*

*Proof.* Since $T_a^2 = \mathrm{id}_Q$ by Lemma 2.7 (see (2.9)), we must have $(b)T_a = b$ or $(b)T_a = b^{-1}$ by the normality of $\langle b \rangle$ in $Q$. If the former situation holds, then $(a^i b^j)T_a = a^i b^j$ for all $i = 0, 1$ and all $j$ since $T_a$ is an automorphism. Therefore $T_a$ fixes every point of $Q$ and hence $a \in C(Q)$. It follows that $(a^i b^j)T_b = a^i b^j$ for all $i = 0, 1$ and all $j$ since $T_b$ is an automorphism. Thus $b \in C(Q)$. Therefore $C(Q) = Q$; that is, $Q$ is commutative, a contradiction. It follows that $(b)T_a = b^{-1}$.

We have that $T_1 = L_{1,1} = L_{1,a} = L_{a,1} = \mathrm{id}_Q$, and so referring to (8.3), we see that the multiplication in $Q$ is entirely determined by the automorphism $L_{a,a} \restriction \langle b \rangle$. If $\langle b \rangle \cong \mathbb{Z}$, then $\mathrm{Aut}(\langle b \rangle) \cong \mathbb{Z}^* = \{\pm 1\}$ and there are two possible values for $L_{a,a} \restriction \langle b \rangle$ determined by $(b)L_{a,a} = b^c$ where $c = \pm 1$. If $\langle b \rangle \cong \mathbb{Z}_n$, then $\mathrm{Aut}(\langle b \rangle) \cong \mathbb{Z}_n^*$, and the possible values for $L_{a,a} \restriction \langle b \rangle$ are given by $(b)L_{a,a} = b^c$ where $c \in \mathbb{Z}_n^*$. In either case, we thus have $(b)L_{a^i,a^k} = b^{c^{ik}}$ for $i, k = 0, 1$.

Fixing $c \in \mathbb{Z}^*$ or $\mathbb{Z}_n^*$, it follows from the preceding discussion that (8.3) specializes to the present setting as follows:

$$a^i b^j \cdot a^k a^\ell = a^{i+k} b^{c^{ij}((-1)^k j + \ell)}\,, \tag{9.4}$$

for all $i, k \in \mathbb{Z}_2$, $j, \ell \in \mathbb{Z}$ or $\mathbb{Z}_n$. Finally, for $m = \infty$ or $2n$, define $\psi : D_m(c) \to Q$ by $(i, j)\psi = a^i b^j$. It is straightforward to check that $\psi$ is an isomorphism using (9.3) and (9.4). □

As an application, we have the following classification results.

**Theorem 9.7.** *Let $Q$ be a finite automorphic loop with a cyclic subgroup of odd order $n$ and of index 2. Then either $Q$ is a cyclic group or $Q \cong D_{2n}(c)$ for some $c \in \mathbb{Z}_n^*$.*

*Proof.* Let $\langle b \rangle$ be a cyclic subgroup of order $n$. This subloop is normal in $Q$ since it has index 2. By Corollary 4.8, $Q$ also has an element $a$ of order 2. By (2.9), $(b)T_a = b$ or $(b)T_a = b^{-1}$, and by the same argument as in the proof of Proposition 9.6, we see that the former case leads to $Q$ being commutative. If $Q$ is commutative, then by [17, Thm. 5.1], $Q$ is isomorphic to the direct product $\mathbb{Z}_2 \times \mathbb{Z}_n \cong \mathbb{Z}_{2n}$. Thus we assume from now on that $Q$ is noncommutative, and so $(b)T_a = b^{-1}$.

It remains to show that $\langle b \rangle$ is the middle nucleus of $Q$. Since $Q$ is the disjoint union of $\langle b \rangle$ and $a\langle b \rangle$, every element of $Q$ has a unique representation in the form $a^i b^j$, $i = 0, 1$, $0 \le j < n$. Thus to show $\langle b \rangle \subseteq N_\mu(Q)$, we must show $(a^i b^j \cdot b^k) \cdot a^\ell b^r = a^i b^j \cdot (b^k \cdot a^\ell b^r)$ for all $0 \le i, \ell \le 1$, $0 \le j, k, r < n$.

Our first step is to prove

$$bab = a\,. \tag{9.5}$$

Set $c = b^{(n+1)/2}$ so that $c^2 = b$. We use (3.4) to get $(x^{-1})P_{xy} = (x^{-1})R_{x^{-1}}^{-1} P_y L_x = xy^2$ for all $x, y \in Q$. Take $x = a/c$ and $y = c$ in this to get $(a/c)b = (a/c)c^2 = [(a/c)^{-1}]P_a = [(a/c)^{-1}]T_a$ because $P_a = T_a$ since $a^2 = 1$. We record this as $(a/c)b = [(a/c)^{-1}]T_a$ and use this identity twice in the following:

$$\begin{aligned} b \cdot (a/c)b &= b \cdot [(a/c)^{-1}]T_a = (b^{-1})T_a \cdot [(a/c)^{-1}]T_a = [b^{-1}(a/c)^{-1}]T_a \\ &= [((a/c)b)^{-1}]T_a = [((a/c)b)T_a]^{-1} = (((a/c)^{-1})T_a T_a)^{-1} = a/c, \end{aligned}$$

where we also used $T_a \in \mathrm{Aut}(Q)$ in the third and fifth equalities, and AAIP in the fourth. Hence $aR_c = aR_cR_bL_b = aR_bL_bR_c$ by Proposition 2.3. Canceling, we obtain (9.5).

Recall that we work under the assumption $(b)T_a = b^{-1}$. By (9.5), we have $a = bab = (a \cdot (b)T_a)b = ab^{-1} \cdot b$. Thus the automorphism $L_aR_bL_a^{-1}R_b^{-1}$ fixes $b^{-1}$ and hence fixes each $b^k$, that is, $ab^k \cdot b = ab^{k+1}$ for $0 \le k < n$. Then the automorphism $L_{b^k}L_aL_{ab^k}^{-1}$ fixes $b$ and hence fixes each $b^r$, that is, $ab^k \cdot b^r = ab^{k+r}$ for $0 \le k, r < n$. Since $ab^k \cdot a = a \cdot b^k a$ (by Proposition 2.3), $L_{b^k}L_aL_{ab^k}^{-1}$ also fixes $a$ and hence fixes each $a^\ell b^r$, that is, $ab^k \cdot a^\ell b^r = a(b^k \cdot a^\ell b^r)$ for $0 \le \ell \le 1$, $0 \le k, r < n$.

On the other hand, by (9.5) again, we have

$$a = bab = b((b)T_a^{-1} \cdot a) = b((b)T_a \cdot a) = b \cdot b^{-1}a.$$

Dualizing the arguments of the preceding paragraph, we get $b^j(b^k \cdot a^\ell b^r) = b^{j+k} \cdot a^\ell b^r$ for $\ell = 0, 1$, $0 \le j, k, r < n$. Combining this with the preceding paragraph, we see that $R_{b^k}R_{a^\ell b^r}R_{b^k \cdot a^\ell b^r}^{-1}$ fixes both $a$ and each $b^j$. It follows that $(a^ib^j \cdot b^k) \cdot a^\ell b^r = a^ib^j \cdot (b^k \cdot a^\ell b^r)$ for $0 \le i, \ell \le 1$, $0 \le j, k, r < n$, as desired.

We have shown that $\langle b \rangle \subseteq N_\mu(Q)$. If $ab^i \in N_\mu(Q)$ for any $i$, then $a \in N_\mu(Q)$ since $N_\mu(Q)$ is a subloop. But then $Q = N_\mu(Q)$, a contradiction. Therefore $\langle b \rangle = N_\mu(Q)$. By Proposition 9.6, we have the desired result. □

Recently, P. Csörgő was able to establish the following result by group-theoretic means.

**Theorem 9.8** (Elementwise Lagrange Theorem [7])**.** *Let $Q$ be a finite automorphic loop and let $a \in Q$. Then the order of $a$ divides the order of $Q$.*

**Corollary 9.9** (Automorphic loops of order $2p$)**.** *Let $Q$ be an automorphic loop of order $2p$ where $p$ is an odd prime. Then $Q \cong D_{2p}(c)$ for some integer $1 \le c < p$, or $Q \cong \mathbb{Z}_{2p}$. Thus there are precisely $p$ automorphic loops of order $2p$, including the cyclic group $\mathbb{Z}_{2p}$ and the dihedral group $D_{2p}$.*

*Proof.* By Corollary 4.8, $Q$ has an element $a$ of order 2. If every element of $Q$ had order 2, then by [15, Thm. 8], $Q$ itself would have order a power of 2, a contradiction. By Theorem 9.8, every element of $Q$ has order dividing $2p$. Thus $Q$ must have an element $b$ of order $p$. Since $\langle a \rangle \cap \langle b \rangle = 1$, the desired isomorphism now follows from Theorem 9.7.

The $p-1$ dihedral automorphic loops $D_{2p}(c)$, $c \in \mathbb{Z}_p^*$, are pairwise nonisomorphic by Corollary 9.4. □

## 10. Open problems

The main open problem in the theory of automorphic loops is the following:

**Problem 10.1.** Does there exist a (finite) simple, nonassociative automorphic loop?

Also open are the Lagrange, Cauchy, Sylow and Hall Theorems.

**Problem 10.2.** Let $Q$ be a finite automorphic loop and let $S \le Q$. Does $|S|$ divide $|Q|$?

**Problem 10.3.** Let $Q$ be a finite automorphic loop.

(i) For each prime $p$ dividing $|Q|$, does $Q$ have an element of order $p$?
(ii) For each prime $p$ dividing $|Q|$, does $Q$ have a Sylow $p$-subloop?
(iii) If $Q$ is solvable and if $\pi$ is a set of primes, does $Q$ have a Hall $\pi$-subloop?

## Acknowledgments

The authors' investigations were aided by the automated deduction tool Prover9 and the finite model builder Mace4, both developed by McCune [22], and the LOOPS package [23] for GAP [12]. The authors thank Ian Wanless for the idea behind the proof of Lemma 4.6(ii). They thank Gábor Nagy for remarking that standard group theory facts about characteristic subgroups should hold for characteristic subloops of automorphic loops.

## References

[1] A. A. Albert, *Quasigroups. I*, Trans. Amer. Math. Soc. **54** (1943), 507–519. MR0009962 (5,229c)
[2] Richard Hubert Bruck, *A survey of binary systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge, Heft 20. Reihe: Gruppentheorie, Springer Verlag, Berlin-Göttingen-Heidelberg, 1958. MR0093552 (20 #76)
[3] R. H. Bruck and Lowell J. Paige, *Loops whose inner mappings are automorphisms*, Ann. of Math. (2) **63** (1956), 308–323. MR0076779 (17,943b)
[4] R. P. Burn, *Finite Bol loops*, Math. Proc. Cambridge Philos. Soc. **84** (1978), no. 3, 377–385. MR0492030 (58 #11194)
[5] Piroska Csörgő, *Multiplication groups of commutative automorphic p-loops of odd order are p-groups*, J. Algebra **350** (2012), 77–83, DOI 10.1016/j.jalgebra.2011.09.038. MR2859876 (2012k:20133)
[6] Piroska Csörgő, *All automorphic loops of order $p^2$ for some prime $p$ are associative*, J. Algebra Appl. **12** (2013), no. 6, 1350013, 8, DOI 10.1142/S0219498813500138. MR3063452
[7] Piroska Csörgő, *All finite automorphic loops have the elementwise Lagrange property*, Rocky Mountain J. Math. **45** (2015), no. 4, 1101–1105. MR3418184
[8] Dylene Agda Souza De Barros, Alexander Grishkov, and Petr Vojtěchovský, *Commutative automorphic loops of order $p^3$*, J. Algebra Appl. **11** (2012), no. 5, 1250100, 15, DOI 10.1142/S0219498812501009. MR2983192
[9] John D. Dixon and Brian Mortimer, *Permutation groups*, Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996. MR1409812 (98m:20003)
[10] Aleš Drápal, *A-loops close to code loops are groups*, Comment. Math. Univ. Carolin. **41** (2000), no. 2, 245–249. Loops'99 (Prague). MR1780868 (2001d:20067)
[11] Tuval Foguel, Michael K. Kinyon, and J. D. Phillips, *On twisted subgroups and Bol loops of odd order*, Rocky Mountain J. Math. **36** (2006), no. 1, 183–212, DOI 10.1216/rmjm/1181069494. MR2228190 (2007d:20115)
[12] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.10; 2007. `http://www.gap-system.org`
[13] George Glauberman, *On loops of odd order*, J. Algebra **1** (1964), 374–396. MR0175991 (31 #267)
[14] George Glauberman, *On loops of odd order. II*, J. Algebra **8** (1968), 393–414. MR0222198 (36 #5250)
[15] Alexander Grishkov, Michael Kinyon, and Gábor P. Nagy, *Solvability of commutative automorphic loops*, Proc. Amer. Math. Soc. **142** (2014), no. 9, 3029–3037, DOI 10.1090/S0002-9939-2014-12053-3. MR3223359
[16] James E. Humphreys, *Introduction to Lie algebras and representation theory*, Graduate Texts in Mathematics, vol. 9, Springer-Verlag, New York-Berlin, 1978. Second printing, revised. MR499562 (81b:17007)
[17] Přemysl Jedlička, Michael Kinyon, and Petr Vojtěchovský, *The structure of commutative automorphic loops*, Trans. Amer. Math. Soc. **363** (2011), no. 1, 365–384, DOI 10.1090/S0002-9947-2010-05088-3. MR2719686 (2011j:20158)

[18] Přemysl Jedlička, Michael K. Kinyon, and Petr Vojtěchovský, *Constructions of commutative automorphic loops*, Comm. Algebra **38** (2010), no. 9, 3243–3267, DOI 10.1080/00927870903200877. MR2724218 (2012c:20190)

[19] Přemysl Jedlička, Michael Kinyon, and Petr Vojtěchovský, *Nilpotency in automorphic loops of prime power order*, J. Algebra **350** (2012), 64–76, DOI 10.1016/j.jalgebra.2011.09.034. MR2859875 (2012j:20190)

[20] Kenneth W. Johnson, Michael K. Kinyon, Gábor P. Nagy, and Petr Vojtěchovský, *Searching for small simple automorphic loops*, LMS J. Comput. Math. **14** (2011), 200–213, DOI 10.1112/S1461157010000173. MR2831230 (2012g:20123)

[21] Michael K. Kinyon, Kenneth Kunen, and J. D. Phillips, *Every diassociative A-loop is Moufang*, Proc. Amer. Math. Soc. **130** (2002), no. 3, 619–624, DOI 10.1090/S0002-9939-01-06090-7. MR1866009 (2002k:20124)

[22] W. W. McCune, *Prover9 and Mace4*, version 2009-11A. `http://www.cs.unm.edu/~mccune/prover9/`

[23] G. P. Nagy and P. Vojtěchovský, *LOOPS: Computing with quasigroups and loops in GAP*, version 2.0.0, computational package for GAP; `http://www.math.du.edu/loops`

[24] J. Marshall Osborn, *A theorem on A-loops*, Proc. Amer. Math. Soc. **9** (1958), 347–349. MR0093555 (20 #79)

[25] Hala O. Pflugfelder, *Quasigroups and loops: introduction*, Sigma Series in Pure Mathematics, vol. 7, Heldermann Verlag, Berlin, 1990. MR1125767 (93g:20132)

[26] D. A. Robinson, *Bol quasigroups*, Publ. Math. Debrecen **19** (1972), 151–153 (1973). MR0325829 (48 #4175)

[27] C. R. B. Wright, *Nilpotency conditions for finite loops*, Illinois J. Math. **9** (1965), 399–409. MR0181691 (31 #5918)

[28] C. R. B. Wright, *On the multiplication group of a loop*, Illinois J. Math. **13** (1969), 660–673. MR0248270 (40 #1522)

Department of Mathematics, University of Denver, Denver, Colorado 80208
*E-mail address*: `mkinyon@du.edu`

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 57306
*E-mail address*: `kunen@math.wisc.edu`

Department of Mathematics and Computer Science, Northern Michigan University, Marquette, Michigan 49855
*E-mail address*: `jophilli@nmu.edu`

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