PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 142, Number 9, September 2014, Pages 3029–3037
S 0002-9939(2014)12053-3
Article electronically published on May 29, 2014

SOLVABILITY OF COMMUTATIVE AUTOMORPHIC LOOPS

ALEXANDER GRISHKOV, MICHAEL KINYON, AND GÁBOR P. NAGY

(Communicated by Pham Huu Tiep)

Abstract. We prove that every finite, commutative automorphic loop is solvable. We also prove that every finite, automorphic 2-loop is solvable. The main idea of the proof is to associate a simple Lie algebra of characteristic 2 to a hypothetical finite simple commutative automorphic loop. The "crust of a thin sandwich" theorem of Zel'manov and Kostrikin leads to a contradiction.

1. Introduction

A *loop* $(Q, \cdot)$ is a set Q with a binary operation $\cdot : Q \times Q \to Q$ such that (i) 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 $x \in Q$. 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 subloop S of a loop Q is *normal* if it is the kernel of a homomorphism; this is equivalent both to S being stabilized under the action of $\mathrm{Inn}(Q)$ and to S being a block of $\mathrm{Mlt}(Q)$ containing 1. A loop Q is *solvable* if it has a subnormal series $1 \leq Q_0 \leq \cdots \leq Q_n = Q$, $Q_i \triangleleft Q_{i+1}$, such that each factor loop Q_{i+1}/Q_i is an abelian group. A loop is *simple* if it has no nontrivial normal subloops. Basic references for loop theory are [3, 17].

A loop is *automorphic* (or an *A-loop*) if every inner mapping is an automorphism, that is, $\mathrm{Inn}(Q) \leq \mathrm{Aut}(Q)$. Automorphic loops were introduced by Bruck and Paige [4]. In recent years, a detailed structure theory has emerged for *commutative* automorphic loops [5, 11–13]. The outstanding open problem in the theory of automorphic loops is the following.

Problem 1. Does there exist a (finite) simple, nonassociative automorphic loop?

It is known that there are no simple nonassociative automorphic loops of order less than 2500 and no simple nonassociative commutative automorphic loops of order less than 2^{12} [14]. The main result of this paper shows that in the commutative case, Problem 1 has a negative answer and, in fact, more than that.

Theorem 2. *Every finite, commutative automorphic loop is solvable.*

For a prime p, a finite loop Q is said to be a *p-loop* if $|Q| = p^m$ for some $m \geq 1$. A by-product of our proof of Theorem 2 is the following.

Received by the editors November 30, 2011 and, in revised form, September 27, 2012 and October 3, 2012.

2010 *Mathematics Subject Classification.* Primary 20N05; Secondary 17B99, 20B15.

Key words and phrases. Automorphic loops, Lie algebras of characteristic 2, primitive groups.

Theorem 3. *Every automorphic 2-loop is solvable.*

Automorphic loops are power-associative; that is, each element generates a (cyclic) group [4]. In particular, every element of an automorphic loop has a two-sided inverse. Unlike the situation for groups, in general power-associative loops, the property of being a p-loop is not equivalent to every element having order a power of p. This is, however, true for automorphic loops. For p odd, this will be found in [15]. In the next section we will show that every finite automorphic loop consisting of elements of 2-power order is a 2-loop. We will address the (elementary) converse in the final section.

We also note that again unlike the group situation, automorphic p-loops are not necessarily nilpotent. Examples of nonnilpotent, commutative, automorphic 2-loops can be found in [12]. Commutative, automorphic p-loops for $p > 2$ are indeed nilpotent, but there exist noncommutative, automorphic loops of order p^3 which are not [13].

Just as for groups, if Q is a loop with normal subloop S, then Q is solvable if and only if both S and Q/S are solvable. Thus, as one would expect, both Theorems 2 and 3 will follow from considering simple loops.

Theorem 2 itself reduces to considering finite simple commutative automorphic loops of exponent 2 because of the following, which is a composite of Theorems 5.1 and 3.12 and Proposition 6.1 of [11].

Proposition 4. *Let Q be a finite, commutative automorphic loop. Then:*

(1) *$Q \cong O(Q) \times E(Q)$, where $|O(Q)|$ is odd and $E(Q)$ is a 2-loop.*
(2) *If $|Q|$ is odd, then Q is solvable.*
(3) *If Q is simple, then Q has exponent 2.*

In particular, suppose Q is a minimal counterexample to Theorem 2. If Q were not simple, then Q would have a normal subloop S such that both Q/S and S are solvable. Since automorphic loops form a variety in the sense of universal algebra [4], both S and Q/S are commutative and automorphic. But this contradicts the nonsolvability of Q. Therefore Q is simple and, by Proposition 4, Q is a 2-loop of exponent 2.

Similarly, suppose Q is a minimal counterexample to Theorem 3. Any subloop and any factor loop of a 2-loop is a 2-loop, and so by the same argument as in the preceding paragraph, it follows that Q is simple. We will show in Theorem 15 that Q must then be commutative and thus by Proposition 4 have exponent 2.

Thus both Theorems 2 and 3 will follow from showing that a finite simple commutative automorphic loop of exponent 2 is a cyclic group of order 2. This will be the main goal of the fourth section.

2. Automorphic 2-loops

In this section, we prove that if every element of a finite automorphic loop has 2-power order, then the loop is a 2-loop.

In a loop Q with two-sided inverses, let $J : Q \to Q; x \mapsto x^{-1}$ denote the inversion map.

Proposition 5 ([14], Corollary 6.6)**.** *Every automorphic loop has the antiautomorphic inverse property; that is, the identity $(xy)^{-1} = y^{-1}x^{-1}$ holds for all x, y. Equivalently, $R_x^J = L_{x^{-1}}$ or $L_x^J = R_{x^{-1}}$ for all x.*

Corollary 6. *If Q is an automorphic loop, then*

$$J \in N_{\mathrm{Sym}(Q)}(\mathrm{Mlt}(Q)) \cap C_{\mathrm{Sym}(Q)}(\mathrm{Inn}(Q)).$$

Proof. That J normalizes $\mathrm{Mlt}(Q)$ follows because $\mathrm{Mlt}(Q)$ is generated by all R_x, L_x. That J centralizes $\mathrm{Inn}(Q)$ follows because $\mathrm{Inn}(Q) \leq \mathrm{Aut}(Q)$, which is centralized by the antiautomorphism J. □

The following result was shown for commutative automorphic loops in [11].

Lemma 7. *Let Q be an automorphic loop. Define the map $P_x = R_x^{-1}L_{x^{-1}} = R_x^{-1}R_x^J$. Then, for all $a, b \in Q$, we have $P_aP_bP_a = P_c$ with $c = bL_{a^{-1}}^{-1}R_a$. Moreover, $P_a^n = P_{a^n}$ holds for all integers n.*

Proof. We have

$$P_aP_bP_a = R_a^{-1}R_a^JR_b^{-1}R_b^JR_a^{-1}R_a^J = g^{-1}g^J,$$

where $g = R_b(R_a^{-1})^JR_a$. Let $c = 1g = bR_a^JR_a = bL_{a^{-1}}^{-1}R_a$ and set $h = gR_c^{-1}$. Observe that $h \in \mathrm{Inn}(Q)$ so that $h \in \mathrm{Aut}(Q)$. Thus

$$P_aP_bP_a = R_c^{-1}h^{-1}JhR_cJ = R_c^{-1}JR_cJ = P_c\,,$$

since h centralizes J. This proves the first statement of the lemma. By putting $a = b^{-1}$, we have $c = a$ and $P_aP_{a^{-1}}P_a = P_a$, which implies $P_{a^{-1}} = P_a^{-1}$. Similarly, $b = 1$ implies $P_{a^2} = P_a^2$. Continuing this, one obtains $P_{a^n} = P_a^n$ for all integers n. □

Theorem 8. *Let Q be a finite automorphic loop. If every element of Q has 2-power order, then Q is a 2-loop.*

Proof. Assume Q is a minimal counterexample. As usual, Q is simple and $\mathrm{Inn}(Q)$ is maximal in $\mathrm{Mlt}(Q)$. Let $G = \mathrm{Mlt}(Q)\langle J\rangle$, let C denote the conjugacy class of J in G and let $X = \{P_x \mid x \in Q\} \subset G$. As J centralizes $\mathrm{Inn}(Q)$, we have $C = \{J^{R_x} \mid x \in Q\}$. Moreover,

$$J^{R_x} = R_x^{-1}JR_x = P_xJ;$$

thus, the map $g \mapsto gJ$ is a bijection between C and X. Take any two elements $J^a, J^b \in C$. As $b = hR_xa$ for some $h \in \mathrm{Inn}(Q)$ and $x \in Q$, we have $J^b = J^{R_xa}$ and $J^bJ^a = (J^{R_x}J)^a = P_x^a$. By Lemma 7, the order of the permutation P_x divides the order of x; thus, the order of J^bJ^a is a power of 2 for all $a, b \in G$ by assumption. The Baer-Suzuki theorem ([16], Thm. 6.7.6) implies that C generates a nilpotent subgroup H of G. As the Sylow 2-group of H is normal in H, H must be a 2-group itself which is normal in G.

If $|H| > 2$, then $H \cap \mathrm{Mlt}(Q)$ is a normal 2-group of $\mathrm{Mlt}(Q)$ whose orbit determines a nontrivial normal subloop of 2-power order, a contradiction. If $|H| = 2$, then $H = \langle J\rangle$ and J is central in G. This implies that Q must be commutative of exponent 2. By ([11, Corollary 6.3]), Q has 2-power order, a contradiction. □

3. The multiplication group of simple automorphic 2-loops

The starting point for our study of simple loops is the following important result, which is an immediate consequence of the characterization of normal subloops as blocks of the multiplication group ([1], Theorem 8).

Proposition 9. *A loop Q is simple if and only if $\mathrm{Mlt}(Q)$ acts primitively on Q.*

The simple loops under consideration here are all 2-loops, and so we will use the classification of primitive groups of degree a power of 2. This follows from the classification of nonabelian simple groups of prime power degree by Guralnick [8] and is stated explicitly in [9]. For $p = 2$, the result can be refined slightly using Zsigmondy's theorem [20] as given in (3.3) of [8].

Recall that a primitive permutation group G is of *affine type* if it has an abelian regular normal subgroup which is necessarily elementary abelian of order p^n for some prime p. In this case G is embedded in the affine group $AGL(n,p)$ with the socle being the translation subgroup. The stabilizer of $0 \in GF(p)^n$ is a subgroup of $GL(n,p)$ which acts irreducibly on $GF(p)^n$.

Proposition 10 (Guralnick and Saxl [9])**.** *Let G be a primitive permutation group of degree 2^n. Then either G is of affine type or G has a unique minimal normal subgroup $N = S \times \cdots \times S = S^t$, $t \geq 1$, S is a nonabelian simple group, and one of the following holds:*

(i) *$S = A_m$, $m = 2^e \geq 8$, $n = te$, and the point stabilizer in N is $N_1 = A_{m-1} \times \cdots \times A_{m-1}$ or*

(ii) *$S = PSL(2,q)$, $q = 2^e - 1 \geq 7$ is a Mersenne prime, $n = te$, and the point stabilizer in N is the direct product of maximal parabolic subgroups, each stabilizing a 1-space.*

We will use the following result of Drápal ([7], Theorem 5.1).

Proposition 11. *Let F be a finite field, $|F| \neq 3, 4$, and let Q be a loop with $\mathrm{Mlt}(Q) \leq P\Gamma L(2,F)$. Then $\mathrm{Mlt}(Q) \cong Q$ is a cyclic group.*

We record one elementary fact about primitive groups.

Lemma 12. *Let G be a permutation group acting primitively on a set Ω. Then for any $x \in \Omega$, G_x acts fixed point freely on $\Omega \setminus \{x\}$.*

Proof. Assume that $y^g = y$ for all $g \in G_x$ and pick $h \in G$ such that $x^h = y$. Then $G_x \leq G_y = G_x^h$ and $h \in N_G(G_x)$. Since G_x is maximal in G, we have $h \in G_x$, and so $y = x$. □

We also need the following consequence of [14, Lemma 4.1].

Lemma 13. *Let Q be a loop and let $H \leq \mathrm{Aut}(Q)$. Then H is not 4-transitive on $Q \setminus \{1\}$.*

We first eliminate all but the case of affine type in Proposition 10.

Theorem 14. *Let Q be a simple automorphic 2-loop. Then $\mathrm{Mlt}(Q)$ is a primitive group of affine type.*

Proof. Suppose $\mathrm{Mlt}(Q)$ is not of affine type. By Proposition 10, $\mathrm{Mlt}(Q)$ contains a unique minimal normal subgroup $N = S^t$, $t \geq 1$, where S is a nonabelian simple group. The subgroup stabilizing $1 \in Q$ is $N_1 = T_{(1)} \times \cdots \times T_{(t)}$, where each $T_{(i)}$ is a maximal subgroup of S. In this case, we can identify Q with the cartesian product $Q_{(1)} \times \cdots \times Q_{(t)}$, where $Q_{(i)}$ is the coset space $S/T_{(i)}$. We write the neutral element of Q in the form $1 = (1, \ldots, 1)$.

Set $Q^* = \{(x, 1, \ldots, 1) \mid x \in Q_{(1)}\}$. Since S acts primitively on each $Q_{(i)}$, Lemma 12 implies that each $T_{(i)}$ acts fixed point freely on $Q_{(i)} \setminus \{1\}$. Thus Q^* is precisely the set of fixed points of the subgroup $1 \times T_{(2)} \times \cdots \times T_{(t)} \leq \mathrm{Inn}(Q)$. Since

$\mathrm{Inn}(Q) \leq \mathrm{Aut}(Q)$, Q^* is a subloop of Q. Let H denote the stabilizer subgroup of Q^* in $\mathrm{Mlt}(Q)$, and let $H^* \leq \mathrm{Sym}(Q^*)$ be the induced permutation group; $H^* \cong H/M$, where M consists of those elements of H acting trivially on Q^*.

By Dedekind's modular law, since $N \lhd \mathrm{Mlt}(Q)$, $\hat{N} = N \cap H = S \times T_{(2)} \times \cdots \times T_{(t)}$ is a normal subgroup of H. Moreover, $M \cap \hat{N} = 1 \times T_{(2)} \times \cdots \times T_{(t)}$ acts trivially on Q^*, and, by $S \cong \hat{N}/(M \cap \hat{N}) \cong M\hat{N}/M$, the induced action of $\hat{N}$ on Q^* is permutation equivalent to the action of S on $Q_{(1)}$. Since $M\hat{N}$ is normal in H, the permutation group H^* on Q^* has $S \times 1 \times \cdots \times 1 \cong S$ as a normal subgroup. Similarly, we can show that $T_{(1)} \times 1 \times \cdots \times 1 \cong T_{(1)} = S_1$ consists of automorphisms of the loop Q^*. After identifying the groups $S \times 1 \times \cdots \times 1$, $T_{(1)} \times 1 \times \cdots \times 1$ with S and $T_{(1)}$, respectively, we have

$$\mathrm{Mlt}(Q^*) \leq H^* \leq N_{\mathrm{Sym}(Q^*)}(S) \qquad \text{and} \qquad T_{(1)} \leq H_1^* \leq \mathrm{Aut}(Q^*). \tag{1}$$

Now assume that case (i) of Proposition 10 holds; that is, $S = A_m$, $T_{(1)} = A_{m-1}$ with $m = 2^e \geq 8$. Then $\mathrm{Aut}(Q^*)$ is 5-transitive on $Q^* \setminus \{1\}$, which is impossible by Lemma 13.

Now assume that case (ii) of Proposition 10 holds; that is, $S = PSL(2, q)$ with $q = 2^e - 1 \geq 7$ a Mersenne prime and each $T_{(i)}$ a maximal parabolic subgroup stabilizing a 1-space. In this case, $N_{\mathrm{Sym}(Q^*)}(PSL(2, q)) = P\Gamma L(2, q)$, and so by (1), $\mathrm{Mlt}(Q^*) \leq P\Gamma L(2, q)$. By Proposition 11, Q^* is a cyclic group. This contradicts the assumption that $T_{(1)} \leq \mathrm{Aut}(Q^*)$ operates transitively on $Q^* \setminus \{1\}$. □

Now we show that like Theorem 2, Theorem 3 reduces to considering commutative automorphic loops of exponent 2.

Theorem 15. *Every simple, automorphic* 2*-loop is commutative of exponent* 2*.*

Proof. Let Q be a simple, automorphic 2-loop. By Theorem 14, $\mathrm{Mlt}(Q)$ is of affine type. Thus $U = \mathrm{soc}(\mathrm{Mlt}(Q))$ is a regular, normal, elementary abelian 2-subgroup. We identify U with a $GF(2)$-vector space and we identify $\mathrm{Inn}(Q)$ with an irreducible subgroup of $GL(U)$. Since U is characteristic in $\mathrm{Mlt}(Q)$, Corollary 6 gives $J \in N_{\mathrm{Sym}(Q)}(U)$. Hence the group $U\langle J\rangle$ is a 2-group, and so $1 \neq Z(U\langle J\rangle) = C_U(J)$. Since J centralizes $\mathrm{Inn}(Q)$, irreducibility of $\mathrm{Inn}(Q)$ gives $C_U(J) = U$, and so $J \restriction U = \mathrm{id}_U$. Thus $J = \mathrm{id}_Q$, and so Q has exponent 2. Then Q is commutative since J is an antiautomorphism (Proposition 5). □

4. Automorphic loops and Lie algebras

We can now prove the main results of the paper by eliminating the case of affine type in Proposition 10. In the proof, we construct a simple Lie algebra from a hypothetical simple commutative automorphic loop of exponent 2. The "crust of a thin sandwich" theorem of Zel'manov and Kostrikin will lead to a contradiction.

Let Q be a finite, simple, commutative, automorphic loop of exponent 2. *We assume from now on* that Q is not associative, and we will work toward a contradiction. Again, $\mathrm{Mlt}(Q)$ is of affine type and we identify $U = \mathrm{soc}(\mathrm{Mlt}(Q))$ with a $GF(2)$-vector space, the operation of which we now write additively. Once again, we identify $\mathrm{Inn}(Q)$ with an irreducible subgroup of $GL(U)$. Each right translation R_x, $x \in Q$, can be factored as $R_x = h_x u_x$ for a unique $h_x \in \mathrm{Inn}(Q)$ and a unique $u_x \in U$.

Set $R_{x,y} = R_x R_y R_{xy}^{-1}$ and note that $R_{x,y} \in \mathrm{Inn}(Q)$. Then

$$R_{x,y} h_{xy} u_{xy} = R_{x,y} R_{xy} = R_x R_y = h_x u_x h_y u_y = h_x h_y (u_x^{h_y} + u_y)\,.$$

Therefore

$$R_{x,y} = h_x h_y h_{xy}^{-1} \qquad \text{and} \qquad u_{xy} = u_x^{h_y} + u_y\,. \tag{2}$$

Now we also have a one-to-one correspondence between U and the set $\{h_x \mid x \in Q\}$. Abusing notation a bit, we may thus index elements of the latter set by elements of U: $h_u = h_x$ where $R_x = h_x u$. This allows us to define an isomorphic copy of Q on U by

$$u \circ v = u^{h_v} + v\,. \tag{3}$$

Denote the right translations in $(U, \circ)$ by $R_u^\circ : v \mapsto v \circ u$, and for $u, v \in U$, set $R_{u,v}^\circ = R_u^\circ R_v^\circ (R_{u\circ v}^\circ)^{-1}$. For all $u, v, w \in U$,

$$\begin{aligned} w R_{u,v}^\circ &= \{[(w^{h_u} + u)^{h_v} + v] + (u^{h_v} + v)\}^{h_{u\circ v}^{-1}} \\ &= \{w^{h_u h_v} + u^{h_v} + v + u^{h_v} + v\}^{h_{u\circ v}^{-1}} = w^{h_u h_v h_{u\circ v}^{-1}}. \end{aligned} \tag{4}$$

Lemma 16. $\mathrm{Inn}(U, \circ) = \mathrm{Inn}(Q) = \langle h_x \mid x \in Q \rangle$.

Proof. (cf. [14], Lemma 6.1)**.** Set $H = \langle h_x \mid x \in Q \rangle$. Since each $h_x \in \mathrm{Inn}(Q)$, $H \leq \mathrm{Inn}(Q)$. Because Q is commutative, $\mathrm{Inn}(Q)$ is generated by the mappings $R_{x,y}$ [2]. By (2), we have $R_{x,y} = h_x h_y h_{xy}^{-1}$, and so $\mathrm{Inn}(Q) = \langle h_x h_y h_{xy}^{-1} \mid x, y \in Q \rangle \leq H$. Similarly, by (4), $\mathrm{Inn}(U, \circ) \leq H$. But $\mathrm{Inn}(Q)$ and $\mathrm{Inn}(U)$ are isomorphic and, hence, by finiteness, equal. □

Lemma 17. *For all $u, v \in U$, $h_u h_v = h_v h_{u^{h_v}}$.*

Proof. Since Q is automorphic, we have for all $u, v, w \in U$,

$$w^{h_v h_{u^{h_v}}} + u^{h_v} = w^{h_v} \circ u^{h_v} = (w \circ u)^{h_v} = (w^{h_u} + u)^{h_v} = w^{h_u h_v} + u^{h_v}\,.$$

The desired result follows immediately. □

Next we define a new binary operation on U as follows:

$$[u, v] = u + v + u \circ v \tag{5}$$

for all $u, v \in U$. Evidently, $[\cdot, \cdot]$ is commutative and $[u, u] = 0$ for all $u \in U$. In addition, $[\cdot, \cdot]$ turns out to be $GF(2)$-bilinear.

Proposition 18 ([18], Theorem 4)**.** $(U, +, [\cdot, \cdot])$ *is a simple, nonassociative algebra over $GF(2)$.*

For $u \in U$, let $\mathrm{ad}(u) : U \to U; v \mapsto [v, u]$ denote the right multiplication mapping in the algebra $(U, +, [\cdot, \cdot])$. We use these notation conventions in anticipation of the following result.

Lemma 19. $(U, +, [\cdot, \cdot])$ *is a simple Lie algebra over $GF(2)$ satisfying*

$$\mathrm{ad}(u)\mathrm{ad}([u, w]) = 0 \tag{6}$$

for all $u, w \in U$.

Proof. We have $(v)\mathrm{ad}(u) = u + v + v^{h_u} + u = v(\mathrm{id}_U + h_u)$; that is,

$$h_u = \mathrm{id}_U + \mathrm{ad}(u)$$

for all $u \in U$. We now use Lemma 17. First we compute

$$h_u h_v = (\mathrm{id}_U + \mathrm{ad}(u))(\mathrm{id}_U + \mathrm{ad}(v)) = \mathrm{id}_U + \mathrm{ad}(u) + \mathrm{ad}(v) + \mathrm{ad}(u)\mathrm{ad}(v)\,.$$

Since $\mathrm{ad}(u + (u)\mathrm{ad}(v)) = \mathrm{ad}(u) + \mathrm{ad}([u, v])$, we also have

$$\begin{aligned} h_v h_{u^{h_v}} &= (\mathrm{id}_U + \mathrm{ad}(v))(\mathrm{id}_U + \mathrm{ad}(u) + \mathrm{ad}([u, v])) \\ &= \mathrm{id}_U + \mathrm{ad}(v) + \mathrm{ad}(u) + \mathrm{ad}(v)\mathrm{ad}(u) + \mathrm{ad}([u, v]) + \mathrm{ad}(v)\mathrm{ad}([u, v])\,. \end{aligned}$$

Equating both expressions, we have

$$\mathrm{ad}(u)\mathrm{ad}(v) = \mathrm{ad}(v)\mathrm{ad}(u) + \mathrm{ad}([u, v]) + \mathrm{ad}(v)\mathrm{ad}([u, v])$$

or, equivalently,

$$\mathrm{ad}(u)\mathrm{ad}(v) + \mathrm{ad}(v)\mathrm{ad}(u) + \mathrm{ad}([u, v]) = \mathrm{ad}(v)\mathrm{ad}([u, v])\,. \tag{7}$$

Since the left side is invariant under switching the roles of u and v, so is the right side, and thus we have

$$\mathrm{ad}(u)\mathrm{ad}([v, u]) = \mathrm{ad}(v)\mathrm{ad}([u, v]) \tag{8}$$

for all $u, v \in U$. Now we linearize (8) by replacing v with $v + w$. We get

$$\begin{aligned} &\mathrm{ad}(u)\mathrm{ad}([v, u]) + \mathrm{ad}(u)\mathrm{ad}([w, u]) \\ &= \mathrm{ad}(v)\mathrm{ad}([u, v]) + \mathrm{ad}(v)\mathrm{ad}([u, w]) + \mathrm{ad}(w)\mathrm{ad}([u, v]) + \mathrm{ad}(w)\mathrm{ad}([u, w])\,. \end{aligned}$$

Using (8) to cancel terms, we obtain

$$\mathrm{ad}(v)\mathrm{ad}([u, w]) + \mathrm{ad}(w)\mathrm{ad}([u, v]) = 0\,.$$

Set $v = u$ and use $[u, u] = 0$ to get

$$\mathrm{ad}(u)\mathrm{ad}([u, w]) = 0\,.$$

This establishes (6). Applying (6) to (7), we have

$$\mathrm{ad}(u)\mathrm{ad}(v) + \mathrm{ad}(v)\mathrm{ad}(u) + \mathrm{ad}([u, v]) = 0\,,$$

which is precisely the Jacobi identity (in characteristic 2). Therefore $(U, +, [\cdot, \cdot])$ is a Lie algebra. The simplicity was already mentioned in Proposition 18. □

For the final step, we will need the important "crust of a thin sandwich" theorem of Zel'manov and Kostrikin [19].

Proposition 20. *Let $\mathfrak{g}$ be a Lie ring generated by a finite collection of elements a satisfying $\mathrm{ad}(a)^2 = 0$ and $\mathrm{ad}(a)\mathrm{ad}(x)\mathrm{ad}(a) = 0$ for all $x \in \mathfrak{g}$. Then $\mathfrak{g}$ is nilpotent.*

Lemma 21. *Let $\mathfrak{g}$ be a Lie ring satisfying (6). If $\mathfrak{g}$ is generated by finitely many elements of the form $[x, y]$, then $\mathfrak{g}$ is nilpotent.*

Proof. We have

$$\mathrm{ad}([x, y])^2 = \mathrm{ad}(x)\mathrm{ad}(y)\mathrm{ad}([x, y]) + \mathrm{ad}(y)\mathrm{ad}(x)\mathrm{ad}([y, x]) = 0\,, \tag{9}$$

by (6). Also,

$$\mathrm{ad}([x, y])\mathrm{ad}(z)\mathrm{ad}([x, y]) = \mathrm{ad}([x, y])^2\mathrm{ad}(z) + \mathrm{ad}([x, y])\mathrm{ad}([z, [x, y]]) = 0\,,$$

using (9) and (6). The conditions of Proposition 20 are satisfied, and so $\mathfrak{g}$ is nilpotent. □

Returning to our Lie algebra $(U, +, [\cdot, \cdot])$, we now obtain a contradiction as follows. Since $(U, +, [\cdot, \cdot])$ is simple, we have $[U, U] = U$. Thus $(U, +, [\cdot, \cdot])$ is generated by finitely many elements of the form $[x, y]$. By Lemmas 19 and 21, $(U, +, [\cdot, \cdot])$ is nilpotent, a contradiction.

We have seen that a simple, commutative, automorphic loop of exponent 2 cannot be nonassociative, and hence must be a cyclic group of order 2. This completes the proofs of Theorem 2 (by Proposition 4) and Theorem 3 (by Theorem 15).

5. Final remarks

We note that the converse of Theorem 8 is an immediate consequence of Theorem 3: if Q is an automorphic 2-loop, then since Q is solvable, it follows from the same argument as in group theory that Q has a subloop S of index 2. We have $x^2 \in S$ for all $x \in Q$, and then by an induction argument, x^2 must have 2-power order. Thus so does x, and hence every element of Q has 2-power order.

A subloop S of a loop Q is *characteristic* if it is invariant under $\mathrm{Aut}(Q)$. Clearly every characteristic subloop of an automorphic loop is normal. In fact, standard facts about characteristic subgroups of groups hold for characteristic subloops of automorphic loops with essentially identical proofs. For instance, a characteristic subloop T of a normal subloop S of an automorphic loop Q is necessarily normal in Q.

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 is characteristic. It follows from the above remarks that if Q is automorphic, then each higher derived subloop Q'', Q''', etc., is normal in Q. In particular, the derived series of a solvable automorphic loop is a *normal* series $Q \trianglerighteq Q' \trianglerighteq Q'' \trianglerighteq \cdots \trianglerighteq Q^{(n)} = 1$.

In a similar vein, we note that a minimal normal subloop of a finite automorphic loop is a direct product of isomorphic simple automorphic loops. Indeed, the same argument that works for groups (*e.g.*, [10], p. 51) applies without change. Thus a minimal normal subloop of a finite solvable automorphic loop is an elementary abelian p-group. These remarks may prove helpful in settling one of the main remaining open problems in the theory of commutative automorphic loops:

Problem 22. Let Q be a commutative automorphic loop. For each prime p, does Q have a Sylow p-subloop? For each set of primes π, does Q have a Hall π-subloop?

References

[1] A. A. Albert, *Quasigroups. I*, Trans. Amer. Math. Soc. **54** (1943), 507–519. MR0009962 (5,229c)

[2] R. H. Bruck, *Contributions to the theory of loops*, Trans. Amer. Math. Soc. **60** (1946), 245–354. MR0017288 (8,134b)

[3] Richard Hubert Bruck, *A survey of binary systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge, Heft 20. Reihe: Gruppentheorie, Springer Verlag, Berlin, 1958. MR0093552 (20 #76)

[4] R. H. Bruck and Lowell J. Paige, *Loops whose inner mappings are automorphisms*, Ann. of Math. (2) **63** (1956), 308–323. MR0076779 (17,943b)

[5] P. Csörgő, *Multiplication groups of commutative automorphic p-loops of odd order are p-groups*, J. Algebra **350** (2012), 77–83. MR2859876 (2012k:20133)

[6] D. A. S. de Barros, A. Grishkov, and P. Vojtěchovský, *Commutative automorphic loops of order p^3*, J. Algebra Appl. **11** (2012), no. 5, 1250100, 15 pp. MR2983192

[7] Aleš Drápal, *Multiplication groups of loops and projective semilinear transformations in dimension two*, J. Algebra **251** (2002), no. 1, 256–278, DOI 10.1006/jabr.2001.9120. MR1900283 (2004a:20073)

[8] Robert M. Guralnick, *Subgroups of prime power index in a simple group*, J. Algebra **81** (1983), no. 2, 304–311, DOI 10.1016/0021-8693(83)90190-4. MR700286 (84m:20007)

[9] Robert M. Guralnick and Jan Saxl, *Monodromy groups of polynomials*, Groups of Lie type and their geometries (Como, 1993), London Math. Soc. Lecture Note Ser., vol. 207, Cambridge Univ. Press, Cambridge, 1995, pp. 125–150, DOI 10.1017/CBO9780511565823.012. MR1320519 (96b:20003)

[10] B. Huppert, *Endliche Gruppen. I* (German), Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin, 1967. MR0224703 (37 #302)

[11] 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)

[12] 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)

[13] 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)

[14] 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)

[15] M. Kinyon, K. Kunen, J. D. Phillips and P. Vojteěchovský, The structure of automorphic loops, Trans. Amer. Math. Soc., to appear.

[16] Hans Kurzweil and Bernd Stellmacher, *The theory of finite groups.* An introduction, translated from the 1998 German original, Universitext, Springer-Verlag, New York, 2004. MR2014408 (2004h:20001)

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

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

[19] E. I. Zel′manov and A. I. Kostrikin, *A theorem on sandwich algebras* (Russian). Translated in Proc. Steklov Inst. Math. **1991**, no. 4, 121–126. Galois theory, rings, algebraic groups and their applications (Russian), Trudy Mat. Inst. Steklov. **183** (1990), 106–111, 225. MR1092020 (92h:17007)

[20] K. Zsigmondy, *Zur Theorie der Potenzreste* (German), Monatsh. Math. Phys. **3** (1892), no. 1, 265–284, DOI 10.1007/BF01692444. MR1546236

Departamento de Matemática, Universidade de São Paulo, Caixa Postal 66281, São Paulo-SP, 05311-970, Brazil

E-mail address: grishkov@ime.usp.br

Department of Mathematics, University of Denver, 2360 S. Gaylord Street, Denver, Colorado 80208

E-mail address: mkinyon@math.du.edu

Bolyai Institute, University of Szeged, Aradi vértanúk tere 1, H-6720 Szeged, Hungary

E-mail address: nagyg@math.u-szeged.hu