NILPOTENCY IN AUTOMORPHIC LOOPS OF PRIME POWER ORDER

PŘEMYSL JEDLIČKA†, MICHAEL KINYON, AND PETR VOJTĚCHOVSKÝ

Abstract. A loop is automorphic if its inner mappings are automorphisms. Using so-called associated operations, we show that every commutative automorphic loop of odd prime power order is centrally nilpotent. Starting with anisotropic planes in the vector space of 2×2 matrices over the field of prime order p, we construct a family of automorphic loops of order p^3 with trivial center.

1. Introduction

A classical result of group theory is that p-groups are (centrally) nilpotent. The analogous result does not hold for loops.

The first difficulty is with the concept of a p-loop. For a prime p, a finite group has order a power of p if and only if each of its elements has order a power of p, so p-groups can be defined in two equivalent ways. Not so for loops, where the order of an element might not be well defined, and even if it is, the two natural p-loop concepts might not be equivalent.

However, there exist several varieties of loops where the analogy with group theory is complete. For instance, a Moufang loop has order a power of p if and only if each of its elements has order a power of p, and, moreover, every Moufang p-loop is nilpotent [7, 8].

We showed in [10, Thm. 7.1] that a finite commutative automorphic loop has order a power of p if and only if each of its elements has order a power of p. The same is true for automorphic loops, by [13], *provided* that p is odd; the case $p = 2$ remains open.

In this paper we study nilpotency in automorphic loops of prime power order. We prove:

Theorem 1.1. *Let p be an odd prime and let Q be a finite commutative automorphic p-loop. Then Q is centrally nilpotent.*

Since there is a (unique) commutative automorphic loop of order 2^3 with trivial center, cf. [9], Theorem 1.1 is best possible in the variety of commutative automorphic loops. (The situation for $p = 2$ is indeed complicated in commutative automorphic loops. By [9, Prop. 6.1], if a nonassociative finite simple commutative automorphic loop exists, it has exponent two. We now know that no nonassociative finite simple commutative automorphic loop of order less than 2^{12} exists [11].)

In fact, Theorem 1.1 is best possible even in the variety of automorphic loops, because for every prime p we construct here a family of automorphic loops of order p^3 with trivial center.

2010 *Mathematics Subject Classification.* Primary: 20N05.

Key words and phrases. automorphic loop, commutative automorphic loop, A-loop, central nilpotency.

† Supported by the Grant Agency of the Czech Republic, grant no. 201/07/P015.

1.1. **Background.** A *loop* $(Q, \cdot)$ is a set Q with a binary operation $\cdot$ such that (i) for each $x \in Q$, the *left translation* $L_x : Q \to Q; y \mapsto yL_x = xy$ and the *right translation* $R_x : Q \to Q; y \mapsto yR_x = yx$ are bijections, and (ii) there exists $1 \in Q$ satisfying $1 \cdot x = x \cdot 1 = x$ for all $x \in Q$.

The left and right translations generate the *multiplication group* $\operatorname{Mlt} Q = \langle L_x, R_x \mid x \in Q \rangle$. The *inner mapping group* $\operatorname{Inn} Q = (\operatorname{Mlt} Q)_1$ is the stabilizer of $1 \in Q$. Standard references for the theory of loops are [1, 2, 18].

A loop Q is *automorphic* (or sometimes just an *A-loop*) if every inner mapping of Q is an automorphism of Q, that is, $\operatorname{Inn} Q \leq \operatorname{Aut} Q$.

The study of automorphic loops was initiated by Bruck and Paige [3]. They obtained many basic results, not the least of which is that automorphic loops are *power-associative*, that is, for all x and all integers m, n, $x^m x^n = x^{m+n}$. In power-associative loops, the *order* of an element may be defined unambiguously.

For commutative automorphic loops, there now exists a detailed structure theory [9], as well as constructions and small order classification results [10].

Informally, the *center* $Z(Q)$ of a loop Q is the set of all elements of Q which commute and associate with all other elements. It can be characterized as $Z(Q) = \operatorname{Fix}(\operatorname{Inn}(Q))$, the set of fixed points of the inner mapping group. (See §2 for the more traditional definition.)

The center is a *normal* subloop of Q, that is, $Z(Q)\varphi = Z(Q)$ for every $\varphi \in \operatorname{Inn} Q$. Define $Z_0(Q) = \{1\}$, and $Z_{i+1}(Q)$, $i \geq 0$, as the preimage of $Z(Q/Z_i(Q))$ under the canonical projection. This defines the *upper central series*

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

of Q. If for some n we have $Z_{n-1}(Q) < Z_n(Q) = Q$ then Q is said to be *(centrally) nilpotent of class n*.

1.2. **Summary.** The proof of our main result, Theorem 1.1, is based on a construction from [9]. On each commutative automorphic loop $(Q, \cdot)$ which is uniquely 2-divisible (*i.e.*, the squaring map $x \mapsto x \cdot x$ is a permutation), there exists a second loop operation $\circ$ such that $(Q, \circ)$ is a Bruck loop (see §3), and such that powers of elements in $(Q, \cdot)$ coincide with those in $(Q, \circ)$.

Glauberman [6] showed that for each odd prime p a finite Bruck p-loop is centrally nilpotent. Theorem 1.1 will therefore follow immediately from this and from the following result:

Theorem 1.2. *Let $(Q, \cdot)$ be a uniquely 2-divisible commutative automorphic loop with associated Bruck loop $(Q, \circ)$. Then $Z_n(Q, \circ) = Z_n(Q, \cdot)$ for every $n \geq 0$.*

After reviewing preliminary results in §2, we discuss the associated Bruck loop in §3 and prove Theorem 1.2 in §4.

In §5, we use anisotropic planes in the vector space of 2×2 matrices over $GF(p)$ to obtain automorphic loops of order p^3 with trivial center. We obtain one such loop for $p = 2$ (this turns out to be the unique commutative automorphic loop of order 2^3 with trivial center), two such loops for $p = 3$, three such loops for $p \geq 5$, and at least one (conjecturally, three) such loop for every prime $p \geq 7$

Finally, we pose open problems in §6.

2. Preliminaries

In a loop $(Q,\cdot)$, there are various subsets of interest:

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

The commutant is not necessarily a subloop, but the nuclei are.

Proposition 2.1. [3] *In an automorphic loop $(Q,\cdot)$, $N_\lambda(Q) = N_\rho(Q) \le N_\mu(Q)$. If, in addition, $(Q,\cdot)$ is commutative, $Z(Q) = N_\lambda(Q)$.*

We will also need the following (well known) characterization of $C(Q)\cap N_\rho(Q)$:

Lemma 2.2. *Let $(Q,\cdot)$ be a loop. Then $a \in C(Q)\cap N_\rho(Q)$ if and only if $L_aL_x = L_xL_a$ for all $x\in Q$.*

Proof. If $a \in C(Q)\cap N_\rho(Q)$, then for all $x,y\in Q$, $a\cdot xy = xy\cdot a = x\cdot ya = x\cdot ay$, that is, $L_aL_x = L_xL_a$. Conversely, if $L_aL_x = L_xL_a$ holds, then applying both sides to 1 gives $xa = ax$, *i.e.*, $a\in C(Q)$, and then $xy\cdot a = a\cdot xy = x\cdot ay = x\cdot ya$, *i.e.*, $a\in N_\rho(Q)$. □

The inner mapping group $\mathrm{Inn}(Q)$ of a loop Q has a standard set of generators

$$L_{x,y} = L_xL_yL_{yx}^{-1},\quad R_{x,y} = R_xR_yR_{xy}^{-1},\quad T_x = L_xR_x^{-1},$$

for x, $y\in Q$. The property of being an automorphic loop can therefore be expressed equationally by demanding that the permutations $L_{x,y}$, $R_{x,y}$, T_x are homomorphisms. In particular, if Q is a commutative loop then Q is automorphic if and only if

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

for every x, y, u, v.

In addition, we can conclude that (commutative) automorphic loops form a variety in the sense of universal algebra, and are therefore closed under subloops, products, and homomorphic images.

We will generally compute with translations whenever possible, but it will sometimes be convenient to work directly with the loop operations. Besides the loop multiplication, we also have the *left division* operation $\backslash : Q\times Q\to Q$ which satisfies

$$x\backslash(xy) = x(x\backslash y) = y\,.$$

The *division permutations* $D_x : Q\to Q$ defined by $yD_x = y\backslash x$ are also quite useful, as is the *inversion permutation* $J : Q\to Q$ defined by $xJ = xD_1 = x^{-1}$.

If Q is a commutative automorphic loop then for all x, $y\in Q$ we have

$$xL_{y,x} = x, \tag{2.1}$$

$$L_{y,x}L_{x^{-1}} = L_{x^{-1}}L_{y,x}, \tag{2.2}$$

$$yL_{y,x} = ((xy)\backslash x)^{-1}, \tag{2.3}$$

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

$$D_{x^2} = D_xJD_x, \tag{2.5}$$

where the first two equalities follow from [9, Lem. 2.3], (2.3) from [9, Lem 2.5], (2.4) is an immediate consequence of [9, Lem. 2.7], and (2.5) is [9, Lem. 2.8]. In addition, commutative automorphic loops satisfy the *automorphic inverse property*

$$(xy)^{-1} = x^{-1}y^{-1} \quad \text{and} \quad (x\backslash y)^{-1} = x^{-1}\backslash y^{-1}, \tag{2.6}$$

by [9, Lem. 2.6].

Finally, as in [9], in a commutative automorphic loop $(Q, \cdot)$, it will be convenient to introduce the permutations

$$P_x = L_x L_{x^{-1}}^{-1} = L_{x^{-1}}^{-1} L_x,$$

where the second equality follows from [9, Lem. 2.3].

Lemma 2.3. *For all x, y in a commutative automorphic loop $(Q, \cdot)$*

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

$$x \cdot xP_y = (xy)^2. \tag{2.8}$$

Proof. Equation (2.7) is from [9, Lem 3.2]. Replacing x with x^{-1} and y with xy in (2.7) yields $xP_{x^{-1}\cdot xy} = x^{-1}(xy)^2$ and $xP_{x^{-1}\cdot xy} = xL_{x,x^{-1}}P_{x^{-1}\cdot xy} = xL_{x,x^{-1}}P_{yL_{x,x^{-1}}}$. Now, for every automorphism φ of Q we have $x\varphi P_{y\varphi} = (y\varphi)^{-1}\backslash(y\varphi x\varphi) = (y^{-1}\backslash(yx))\varphi = xP_y\varphi$. Thus $x^{-1}(xy)^2 = xL_{x,x^{-1}}P_{yL_{x,x^{-1}}} = xP_yL_{x,x^{-1}}$. Canceling x^{-1} on both sides, we obtain (2.8). □

3. The associated Bruck loop

A loop $(Q, \circ)$ is said to be a (left) *Bol loop* if it satisfies the identity

$$(x \circ (y \circ x)) \circ z = x \circ (y \circ (x \circ z)). \tag{3.1}$$

A Bol loop is a *Bruck loop* if it also satisfies the automorphic inverse property $(x \circ y)^{-1} = x^{-1} \circ y^{-1}$. (Bruck loops are also known as *K-loops* or *gyrocommutative gyrogroups*.)

The following construction is the reason for considering Bruck loops in this paper. Let $(Q, \cdot)$ be a uniquely 2-divisible commutative automorphic loop. Define a new operation $\circ$ on Q by

$$x \circ y := [x^{-1}\backslash(xy^2)]^{1/2} = [(y^2)P_x]^{1/2}.$$

By [9, Lem. 3.5], $(Q, \circ)$ is a Bruck loop, and powers in $(Q, \circ)$ coincide with powers in $(Q, \cdot)$.

Since we will work with translations in both $(Q, \cdot)$ and $(Q, \circ)$, we will denote left translations in $(Q, \circ)$ by L_x°. For instance, we can express the fact that every Bol loop $(Q, \circ)$ is *left power alternative* by

$$(L_x^\circ)^n = L_{x^n}^\circ \tag{3.2}$$

for all integers n.

Proposition 3.1. [12, Thm. 5.10] *Let $(Q, \circ)$ be a Bol loop. Then $N_\lambda(Q, \circ) = N_\mu(Q, \circ)$. If, in addition, $(Q, \circ)$ is a Bruck loop, then $N_\lambda(Q, \circ) = Z(Q, \circ)$.*

In the uniquely 2-divisible case, we can say more about the center.

Lemma 3.2. *Let $(Q, \circ)$ be a uniquely 2-divisible Bol loop. Then $Z(Q, \circ) = C(Q, \circ) \cap N_\rho(Q, \circ)$.*

Proof. One inclusion is obvious. For the other, suppose $a \in C(Q,\circ) \cap N_\rho(Q,\circ)$. Then for all $x, y \in Q$,

$$\begin{aligned}(x^2 \circ a) \circ y &\overset{(3.2)}{=} (x \circ (x \circ a)) \circ y = (x \circ (a \circ x)) \circ y \\ &\overset{(3.1)}{=} x \circ (a \circ (x \circ y)) = x \circ (x \circ (a \circ y)) \\ &\overset{(3.2)}{=} x^2 \circ (a \circ y)\,,\end{aligned}$$

where we used $a \in C(Q,\circ)$ in the second equality and Lemma 2.2 in the fourth. Since squaring is a permutation, we may replace x^2 with x to get $(x \circ a) \circ y = x \circ (a \circ y)$ for all $x, y \in Q$. Thus $a \in N_\mu(Q,\circ) = N_\lambda(Q,\circ)$ (Proposition 3.1), and so $a \in Z(Q,\circ)$. □

Lemma 3.3. *Let $(Q,\cdot)$ be a uniquely 2-divisible commutative automorphic loop with associated Bruck loop $(Q,\circ)$. Then $a \in Z(Q,\circ)$ if and only if, for all $x \in Q$,*

$$P_a P_x = P_x P_a\,. \tag{3.3}$$

Proof. By Lemmas 2.2 and 3.2, $a \in Z(Q,\circ)$ if and only if the identity $a \circ (x \circ y) = x \circ (a \circ y)$ holds for all $x, y \in Q$. This can be written as $[(y^2)P_x P_a]^{1/2} = [(y^2)P_a P_x]^{1/2}$. Squaring both sides and using unique 2-divisibility to replace y^2 with y, we have $(y)P_x P_a = (y)P_a P_x$ for all $x, y \in Q$. □

4. Proofs of the Main Results

Throughout this section, let $(Q,\cdot)$ be a uniquely 2-divisible, commutative automorphic loop with associated Bruck loop $(Q,\circ)$.

Lemma 4.1. *If $a \in Z(Q,\circ)$, then for all $x \in Q$,*

$$xL_{a\backslash x,a} = xL_{a\backslash x^{-1},a}\,. \tag{4.1}$$

Proof. First,

$$\begin{aligned}x^{-2} = x^{-2}L^{-1}_{a^{-1}}L_{a^{-1}} \quad &= a^{-1}D_{x^{-2}}L_{a^{-1}} \\ \overset{(2.6)}{=} aD_{x^2}JL_{a^{-1}} \quad &\overset{(2.5)}{=} aD_xJD_xJL_{a^{-1}} \\ \overset{(2.6)}{=} aD_xD_{x^{-1}}L_{a^{-1}} &= (x^{-1})L^{-1}_{a\backslash x}L_{a^{-1}}\,.\end{aligned}$$

Thus we compute

$$\begin{aligned}(x^{-2})L_{a\backslash x,a} = (x^{-1})L^{-1}_{a\backslash x}L_{a^{-1}}L_{a\backslash x,a} &\overset{(2.2)}{=} (x^{-1})L^{-1}_{a\backslash x}L_{a\backslash x,a}L_{a^{-1}} \\ = (x^{-1})L_aL_x^{-1}L_{a^{-1}} \quad &= aL_{x^{-1}}L_x^{-1}L_{a^{-1}} \\ = aP_{x^{-1}}L_{a^{-1}}\,,\end{aligned} \tag{4.2}$$

Since $a^{-1} \in Z(Q,\circ)$, we may also apply (4.2) with a^{-1} in place of a, and will do so in the next calculation. Now

$$\begin{aligned}aP_{x^{-1}}L_{a^{-1}} = aP_{x^{-1}}P_{a^{-1}}L_a \quad &\overset{(3.3)}{=} aP_{a^{-1}}P_{x^{-1}}L_a \\ = a^{-1}P_{x^{-1}}L_a \quad &\overset{(4.2)}{=} (x^{-2})L_{a^{-1}\backslash x,a^{-1}} \\ \overset{(2.6)}{=} (x^{-2})L_{(a\backslash x^{-1})^{-1},a^{-1}} \quad &\overset{(2.4)}{=} (x^{-2})L_{a\backslash x^{-1},a}\,,\end{aligned}$$

where we used $a^{-1} \in Z(Q, \circ)$ in the second equality.

Putting this together with (4.2), we have $(x^{-2})L_{a\backslash x,a} = (x^{-2})L_{a\backslash x^{-1},a}$ for all $x \in Q$. Since inner mappings are automorphisms, this implies $(xL_{a\backslash x,a})^{-2} = (xL_{a\backslash x^{-1},a})^{-2}$. Taking inverses and square roots, we have the desired result. □

Lemma 4.2. *If $a \in Z(Q, \circ)$, then for all $x \in Q$,*

$$(a\backslash x)L_{a\backslash x^{-1},a} = (x\backslash a)^{-1}, \tag{4.3}$$

$$x^{-1} \cdot xP_a = a^2. \tag{4.4}$$

Proof. We compute

$$(a\backslash x)L_{a\backslash x^{-1},a} = a\backslash(xL_{a\backslash x^{-1},a}) \overset{(4.1)}{=} a\backslash(xL_{a\backslash x,a}) \overset{(2.1)}{=} (a\backslash x)L_{a\backslash x,a} \overset{(2.3)}{=} (x\backslash a)^{-1}\,,$$

where we used $L_{a\backslash x^{-1},a} \in \mathrm{Aut}(Q)$ in the first equality and $L_{a\backslash x,a} \in \mathrm{Aut}(Q)$ in the third equality.

To show (4.4), we compute

$$\begin{aligned}
x^{-1} \cdot xP_a &= (x^{-1})L_{a^{-1}\backslash(ax)} && = (x^{-1})L_{a^{-1}\backslash(ax)}L_{a^{-1}}L_{ax}^{-1}L_{ax}L_{a^{-1}}^{-1} \\
&= (a\backslash(ax))^{-1}L_{a^{-1}\backslash(ax),a^{-1}}L_{ax}L_{a^{-1}}^{-1} && \overset{(2.6)}{=} (a^{-1}\backslash(ax)^{-1})L_{a^{-1}\backslash(ax),a^{-1}}L_{ax}L_{a^{-1}}^{-1} \\
&\overset{(4.3)}{=} ((ax)^{-1}\backslash a^{-1})^{-1}L_{ax}L_{a^{-1}}^{-1} && \overset{(2.6)}{=} ((ax)\backslash a)L_{ax}L_{a^{-1}}^{-1} \\
&= aL_{a^{-1}}^{-1} && = a^2\,.
\end{aligned}$$

Note that in the fifth equality, we are applying (4.3) with a^{-1} in place of a and $(ax)^{-1}$ in place of x. □

Lemma 4.3. *If $a \in Z(Q, \circ)$, then $L_a = L_a^\circ$, and for all integers n*

$$L_a^n = L_{a^n}. \tag{4.5}$$

Proof. For $x \in Q$, we compute

$$(a \circ x)^2 = (x \circ a)^2 = (a^2)P_x \overset{(4.4)}{=} xP_aL_{x^{-1}}P_x = x \cdot xP_a \overset{(2.8)}{=} (ax)^2\,.$$

Taking square roots, we have $a \circ x = ax$, as desired. Then $L_a^n = (L_a^\circ)^n \overset{(3.2)}{=} L_{a^n}^\circ = L_{a^n}$. □

Lemma 4.4. *If $a \in Z(Q, \circ)$, then for all $x \in Q$,*

$$P_{xa} = P_xP_a\,. \tag{4.6}$$

Proof. For each $y \in Q$,

$$yP_{xa} = yP_{ax} = [ax \circ y^{1/2}]^2 = [(a \circ x) \circ y^{1/2}]^2 = [a \circ (x \circ y^{1/2})]^2 = yP_xP_a\,,$$

using Lemma 4.3 in the third equality and $a \in Z(Q, \circ)$ in the fourth. □

Lemma 4.5. *If $a \in Z(Q, \circ)$, then $a^2 \in Z(Q, \cdot)$.*

Proof. We compute

$$\begin{aligned} L_{a^2}L_x &\overset{(4.5)}{=} L_a^2 L_x && = L_a L_{a,x} L_{xa} \\ &\overset{(2.4)}{=} L_a L_{a^{-1},x^{-1}} L_{xa} && = L_a L_{a^{-1}} L_{x^{-1}} L^{-1}_{x^{-1}a^{-1}} L_{xa} \\ &\overset{(4.5)}{=} L_{x^{-1}} L^{-1}_{x^{-1}a^{-1}} L_{xa} && \overset{(2.6)}{=} L_{x^{-1}} L^{-1}_{(xa)^{-1}} L_{xa} \\ &= L_{x^{-1}} P_{xa} && \overset{(4.6)}{=} L_{x^{-1}} P_x P_a \\ &= L_x L_a L^{-1}_{a^{-1}} && \overset{(4.5)}{=} L_x L_a^2 \\ &\overset{(4.5)}{=} L_x L_{a^2} . \end{aligned}$$

By Lemma 2.2, it follows that $a^2 \in N_\rho(Q,\cdot)$, and $N_\rho(Q,\cdot) = Z(Q,\cdot)$ by Proposition 2.1. □

Lemma 4.6. *Let $(Q,\cdot)$ be a uniquely 2-divisible commutative automorphic loop with associated Bruck loop $(Q,\circ)$. Then $Z(Q,\circ) \subset Z(Q,\cdot)$.*

Proof. Assume that $a \in Z(Q,\circ)$. Then $a^2 \in Z(Q,\cdot)$ by Lemma 4.5, and thus $(aL_{x,y})^2 = a^2 L_{x,y} = a^2$ for every x, $y \in Q$. Taking square roots yields $aL_{x,y} = a$, that is, $a \in Z(Q,\cdot)$. □

Now we prove Theorem 1.2, that is, we show that the upper central series of $(Q,\cdot)$ and $(Q,\circ)$ coincide.

Proof of Theorem 1.2. Since each $Z_n(Q)$ is the preimage of $Z(Q/Z_{n-1}(Q))$ under the canonical projection, it follows by induction that it suffices to show $Z(Q,\circ) = Z(Q,\cdot)$. One inclusion is Lemma 4.6. For the other, suppose $a \in Z(Q,\cdot)$. Then $P_a P_x = L_a L^{-1}_{a^{-1}} L_x L^{-1}_{x^{-1}} = L_x L^{-1}_{x^{-1}} L_a L^{-1}_{a^{-1}} = P_x P_a$, and so $a \in Z(Q,\circ)$ by Lemma 3.3. □

Proof of Theorem 1.1. For an odd prime p, let Q be a commutative automorphic p-loop with associated Bruck loop $(Q,\circ)$. By [6], $(Q,\circ)$ is centrally nilpotent of class, say, n. By Theorem 1.2, Q is also centrally nilpotent of class n. □

5. From anisotropic planes to automorphic p-loops with trivial nucleus

We proved in [10] that a commutative automorphic loop of order p, $2p$, $4p$, p^2, $2p^2$ or $4p^2$ is an abelian group. For every prime p there exist nonassociative commutative automorphic loops of order p^3. These loops have been classified up to isomorphism in [4], where the announced Theorem 1.1 has been used to guarantee nilpotency for p odd.

Without commutativity, we do not even know whether automorphic loops of order p^2 are associative! Nevertheless we show here that the situation is much more complicated than in the commutative case already for loops of order p^3. Namely, using anisotropic planes in the vector space $M(2,p)$ of 2×2 matrices over $GF(p)$, we construct a family of automorphic loops of order p^3 with trivial center.

5.1. **Anisotropic planes.** Let F be a field and $M(2,F)$ the vector space of 2×2 matrices over F. The determinant

$$\det : M(2,F) \to F, \quad \det \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = a_1 a_4 - a_2 a_3$$

is a quadratic form.

Recall that a subspace W of $M(2,F)$ is *anisotropic* if $\det(A) \neq 0$ for every $0 \neq A \in W$. An anisotropic subspace of dimension two is called an *anisotropic plane*.

If $FC \oplus FD$ is an anisotropic plane in $M(2,F)$ then $C^{-1}(FC \oplus FD)$ is also anisotropic, and hence, while looking for anisotropic planes, it suffices to consider subspaces $FI \oplus FA$, where I is the identity matrix and $A \in GL(2,F)$.

Lemma 5.1. *With $A \in M(2,F)$, the subspace $FI \oplus FA$ is an anisotropic plane if and only if the characteristic polynomial $\det(A - \lambda I) = \lambda^2 - \mathrm{tr}(A)\lambda + \det(A)$ has no roots in F.*

Proof. The subspace $FI \oplus FA$ is anisotropic if and only if $\det(\lambda I + \mu A) \neq 0$ for every λ, μ such that $(\lambda, \mu) \neq (0,0)$, or, equivalently, if and only if $\det(A - \lambda I) \neq 0$ for every λ. We have $\det(A - \lambda I) = \lambda^2 - \mathrm{tr}(A)\lambda + \det(A)$. □

If F is algebraically closed, the characteristic polynomial of Lemma 5.1 will have roots and hence there are no anisotropic planes in $M(2,F)$. But it is easy to construct anisotropic planes in $M(2,\mathbb{R})$, for instance, by making sure that the discriminant $\mathrm{tr}(A)^2 - 4\det(A)$ is negative. We are now going to show that there are anisotropic planes (with additional properties) over every finite prime field.

A nonzero element $a \in GF(p)$ is a *quadratic residue* if $a = b^2$ for some $b \in GF(p)$. A nonzero element $a \in GF(p)$ that is not a quadratic residue is a *quadratic nonresidue*.

To guarantee existence of certain anisotropic planes we will need Lemma 5.3, which can easily be proved from the following strong results of Perron [16, Thms. 1 and 3] concerning additive properties of the set of quadratic residues:

Theorem 5.2. [16] *Let p be a prime, N_p the set of quadratic nonresidues, and $R_p = \{a \in GF(p);\ a$ is a quadratic residue or $a = 0\}$.*

(i) If $p = 4k-1$ and $a \neq 0$ then $|(R_p + a) \cap R_p| = k = |(R_p + a) \cap N_p|$.
(ii) If $p = 4k+1$ and $a \neq 0$ then $|(R_p + a) \cap R_p| = k+1$, $|(R_p + a) \cap N_p| = k$.

Lemma 5.3. *For every prime $p \geq 7$ and every $a \neq 0$ there are $\lambda \neq 0$ and $\mu \neq 0$ such that $\lambda^2 + a$ is a quadratic residue and $\mu^2 + a$ is quadratic nonresidue.*

Proof. We will use Theorem 5.2 without reference. Let $p = 4k \pm 1$. If $k \geq 3$ then $|(R_p + a) \cap R_p| \geq 3$, so there is $\lambda \neq 0$ such that $0 \neq \lambda^2 + a \in R_p$. If $k \geq 2$ then $|(R_p + a) \cap N_p| \geq 2$, and since $0 \notin N_p$, there is $\lambda \neq 0$ such that $\lambda^2 + a \in N_p$. □

Lemma 5.4. *Let p be a prime and $F = GF(p)$.*

(i) There is $A \in GL(2,p)$ such that $\mathrm{tr}(A) = 0$ and $FI \oplus FA$ is anisotropic if and only if $p \neq 2$.
(ii) There is $A \in GL(2,p)$ such that $\mathrm{tr}(A) \neq 0$, $\det(A)$ is a quadratic residue modulo p and $FI \oplus FA$ is anisotropic if and only if $p \neq 3$.
(iii) There is $A \in GL(2,p)$ such that $\mathrm{tr}(A) \neq 0$, $\det(A)$ is a quadratic nonresidue modulo p and $FI \oplus FA$ is anisotropic if and only if $p \neq 2$.

Proof. (i): If $p \geq 3$, let a be a quadratic nonresidue and let

$$A = \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}.$$

Then $\mathrm{tr}(A) = 0$ and $\det(A - \lambda I) = \lambda^2 + \det(A) = \lambda^2 - a$ has no roots, so $FI \oplus FA$ is anisotropic by Lemma 5.1.

If $p = 2$, the only elements $A \in GL(2,p)$ with $\mathrm{tr}(A) = 0$ are

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Then $\det(A + I) = 0$, so $FI \oplus FA$ is not anisotropic by Lemma 5.1.

(ii) and (iii): Let $p \geq 3$ and let a and A be as above. For $\lambda \neq 0$ let

$$B_\lambda = A - \lambda I = \begin{pmatrix} -\lambda & 1 \\ a & -\lambda \end{pmatrix}.$$

Then $FI \oplus FB_\lambda = FI \oplus FA$ is anisotropic, $\mathrm{tr}(B_\lambda) = -2\lambda \neq 0$, and $\det(B_\lambda) = \lambda^2 - a$. If $p \geq 7$, Lemma 5.3 implies that there are $\lambda \neq 0$ and $\mu \neq 0$ such that $\det(B_\lambda)$ is a quadratic residue and $\det(B_\mu)$ is a quadratic nonresidue. If $p = 5$, the two matrices

$$C = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 1 \\ 3 & 1 \end{pmatrix}$$

are of the form B_λ with a suitable choice of a quadratic nonresidue a and a nonzero scalar λ. Moreover, $\mathrm{tr}(C) = \mathrm{tr}(D) \neq 0$, $\det(C) = 4$ is a quadratic residue and $\det(D) = 3$ is a quadratic nonresidue. If $p = 3$, the matrix C is again of the form B_λ for a suitable a and λ, $\mathrm{tr}(C) \neq 0$ and $\det(C) = 2$ is a quadratic nonresidue.

Let $p = 3$ and assume that E satisfies $\mathrm{tr}(E) \neq 0$, $\det(E)$ is a quadratic residue. Then $\det(E) = 1$, and $\det(E - \lambda I)$ is either $\lambda^2 + \lambda + 1$ (with root $\lambda = 1$) or $\lambda^2 - \lambda + 1$ (with root $\lambda = -1$), so $FI \oplus FE$ is not anisotropic by Lemma 5.1.

Finally assume that $p = 2$. Since every nonzero element of $GF(2)$ is a quadratic residue, we have (iii). On the other hand,

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

satisfies the conditions of (ii). □

5.2. **Automorphic loops of order p^3 with trivial nucleus.** Let $A \in GL(2,p)$ be such that $FI \oplus FA$ is an anisotropic plane. Define a binary operation on $F \times (F \times F)$ by

$$(a, x) \cdot (b, y) = (a + b, x(I + bA) + y(I - aA)) \tag{5.1}$$

and call the resulting groupoid $Q(A)$. Since

$$U_a = I + aA$$

is invertible for every $a \in F$, we see that $Q(A)$ is a loop (see Remark 5.8), and in fact, straightforward calculation shows that

$$(b, y)L^{-1}_{(a,x)} = (b - a, (y - xU_{b-a})U^{-1}_{-a}),$$
$$(b, y)R^{-1}_{(a,x)} = (b - a, (y - xU_{a-b})U^{-1}_{a}).$$

Lemma 5.5. *Let $F = GF(p)$. Let $A \in GL(2,p)$ be such that $FI \oplus FA$ is an anisotropic plane in $M(2,p)$. For each $z \in F \times F$ and each $C \in GL(2,p)$ satisfying $CA = AC$, define $\varphi_{z,C} : F \times (F \times F) \to F \times (F \times F)$ by*

$$(a, x)\varphi_{z,C} = (a, az + xC).$$

Then $\varphi_{z,C}$ is an automorphism of $Q(A)$.

Proof. We compute

$$\begin{aligned}(a,x)\varphi_{z,C}\cdot(b,y)\varphi_{z,C} &= (a,az+xC)\cdot(b,bz+yC)\\ &= (a+b,(az+xC)U_b+(bz+yC)U_{-a})\\ &= (a+b,(a+b)z+xCU_b+yCU_{-a}+abzA-abzA)\\ &= (a+b,(a+b)z+(xU_b+yU_{-a})C)\\ &= [(a,x)\cdot(b,y)]\varphi_{z,C}\,,\end{aligned}$$

where we have used $CA=AC$ in the fourth equality. Since $\varphi_{z,C}$ is clearly a bijection, we have the desired result. □

Proposition 5.6. *Let $F=GF(p)$. Let $A\in GL(2,p)$ be such that $FI\oplus FA$ is an anisotropic plane in $M(2,p)$. Then the loop $Q=Q(A)$ is an automorphic loop of order p^3 and exponent p with $N_\mu(Q)=\{(0,x)\,|\,x\in F\times F\}\cong F\times F$ and $N_\lambda(Q)=N_\rho(Q)=1$. In particular, $N(Q)=Z(Q)=1$ and so Q is not centrally nilpotent. In addition, if $p=2$ then $C(Q)=Q$, while if $p>2$, then $C(Q)=1$.*

Proof. Easy calculations show that the standard generators of the inner mapping group of $Q(A)$ are

$$\begin{aligned}(b,y)T_{(a,x)} &= (b,(x(U_{-b}-U_b)+yU_a)U_{-a}^{-1})\,,\\ (c,z)R_{(a,x),(b,y)} &= (c,(zU_aU_b+y(U_{-c-a}-U_{-c}U_{-a}))U_{a+b}^{-1})\,,\\ (c,z)L_{(a,x),(b,y)} &= (c,(zU_{-a}U_{-b}+y(U_{c+a}-U_cU_a))U_{-a-b}^{-1})\,.\end{aligned}\tag{5.2}$$

Since $U_{-b}-U_b=-2bA$ and $U_{c+a}-U_cU_a=U_{-c-a}-U_{-c}U_{-a}=-caA^2$, we find that each of these generators is of the form $\varphi_{u,C}$ for an appropriate $u\in F\times F$, $C\in GL(2,p)$ commuting with A. Specifically, we have

$$\begin{aligned}T_{(a,x)}=\varphi_{u,C} &\quad\text{where}\quad u=-2xAU_{-a}^{-1} &&\text{and}\quad C=U_aU_{-a}^{-1}\,,\\ R_{(a,x),(b,y)}=\varphi_{u,C} &\quad\text{where}\quad u=-ayA^2U_{a+b}^{-1} &&\text{and}\quad C=U_aU_bU_{a+b}^{-1}\,,\\ L_{(a,x),(b,y)}=\varphi_{u,C} &\quad\text{where}\quad u=-ayA^2U_{-a-b}^{-1} &&\text{and}\quad C=U_{-a}U_{-b}U_{-a-b}^{-1}\,.\end{aligned}$$

By Lemma 5.5, it follows that $Q(A)$ is automorphic.

An easy induction shows that powers in $Q(A)$ and in $F\times(F\times F)$ coincide, so $Q(A)$ has exponent p.

Suppose that $(a,x)\in N_\mu(Q)$. Then $(c,z)R_{(a,x),(y,b)}=(c,z)$ for every $(c,z),(b,y)$. Thus $(zU_bU_a+y(U_{-c-a}-U_{-c}U_{-a}))U_{a+b}^{-1}=z$ for every $(c,z),(b,y)$. With $z=0$, we have $y(U_{-c-a}-U_{-c}U_{-a})=-cayA^2=0$ for every y, hence $caA^2=0$ for every c, and $a=0$ follows. On the other hand, clearly $(0,x)\in N_\mu(Q)$ for every x. We have thus shown $N_\mu(Q)=\{(0,x)\,|\,x\in F\times F\}\cong F\times F$.

Suppose that $(c,z)\in N_\lambda(Q)$. Then $(c,z)R_{(a,x),(y,b)}=(c,z)$ for every $(a,x),(b,y)$. Thus $(zU_bU_a+y(U_{-c-a}-U_{-c}U_{-a}))U_{a+b}^{-1}=z$ for every $(a,x),(b,y)$. With $y=0$, we deduce that $zU_{a+b}=zU_aU_b$, or $abzA^2=0$ for every a,b. In particular, $zA^2=0$, and $z=0$ follows. Then $y(U_{-c-a}-U_{-c}U_{-a})=-cayA^2=0$ for every y, hence $caA^2=0$ for every a, and $c=0$ follows. We have proved that $N_\lambda(Q)=1$, and since $Q(A)$ is automorphic, $N_\rho(Q)=1$ as well by Proposition 2.1.

If $p = 2$, then since $U_a = U_{-a}$, it follows that Q is commutative. Now assume that $p > 2$ and let $(a, x) \in C(Q)$. Then $x(U_b - U_{-b}) = y(U_a - U_{-a})$, that is, $2bxA = 2ayA$ for every $(b, y) \in Q$. With $b = 0$ we deduce that $2ayA = 0$ for every y, thus $0 = 2aA$, or $a = 0$. Then $2bxA = 0$, and with $b = 1$ we deduce $2xA = 0$, or $x = 0$. We have proved that $C(Q) = 1$. $\square$

Remark 5.7. The construction $Q(A)$ works for every real anisotropic plane $\mathbb{R}I \oplus \mathbb{R}A$ and results in an automorphic loop on $\mathbb{R}^3$ with trivial center. We believe that this is the first time a smooth nonassociative automorphic loop has been constructed.

Remark 5.8. The groupoid $Q(A)$ is an automorphic loop as long as $I + aA$ is invertible for every $a \in F$, which is a weaker condition than having $FI \oplus FA$ an anisotropic plane, as witnessed by $A = 0$, for instance.

Let us assume that $A \in M(2, F)$ is such that $I + aA$ is invertible for every $a \neq 0$ but $FI \oplus FA$ is not anisotropic. Then $\det(A) = 0$ and $\det(A - \lambda I) = \lambda^2 - \mathrm{tr}(A)\lambda = \lambda(\lambda - \mathrm{tr}(A))$ has no nonzero solutions. Hence $\mathrm{tr}(A) = 0$, and there are $u \in F$ and $0 \neq v \in F$ such that

$$A = \begin{pmatrix} u & v \\ -\frac{u^2}{v} & -u \end{pmatrix} \quad \text{or} \quad A = \begin{pmatrix} u & -\frac{u^2}{v} \\ v & -u \end{pmatrix}. \tag{5.3}$$

In particular, $A^2 = 0$. The loop $Q = Q(A)$ is still an automorphic loop by the argument given in the proof of Proposition 5.6, and we claim that it is a group. Indeed, we have $(c, z) \in N_\lambda(Q) = N(Q)$ if and only if $(c, z) = (c, z)R_{(a,x),(b,y)}$ for every (a, x), (b, y), that is, by (5.2),

$$z = (zU_aU_b + y(U_{-c-a} - U_{-c}U_{-a}))U_{a+b}^{-1} \tag{5.4}$$

for every (a, x), (b, y). As $U_{b+a} - U_bU_a = -baA^2 = 0$ for every a, b, we see that equation (5.4) holds, $(c, z) \in N(Q)$, and Q is a group.

6. Open problems

Problem 6.1. *Are the following two statements equivalent for a finite automorphic loop Q?*

(i) Q has order a power of 2.

(ii) Every element of Q has order a power of 2.

Problem 6.2. *Let p be a prime. Are all automorphic loops of order p^2 associative?*

Problem 6.3. *Let p be a prime. Is there an automorphic loop of order a power of p and with trivial middle nucleus?*

Problem 6.4. *Let p be a prime. Are there automorphic loops of order p^3 that are not centrally nilpotent and that are not constructed by Proposition 5.6?*

Conjecture 6.5. *Let p be a prime and $F = GF(p)$. Call an element $A \in GL(2, p)$ of* type 1 *if $\mathrm{tr}(A) = 0$, of* type 2 *if $\mathrm{tr}(A) \neq 0$ and $\det(A)$ is a quadratic residue, and of* type 3 *if $\mathrm{tr}(A) \neq 0$ and $\det(A)$ is a quadratic nonresidue.*

Let A, $B \in GL(2, p)$ be such that $FI \oplus FA$ and $FI \oplus FB$ are anisotropic planes. Then the loops $Q(A)$, $Q(B)$ constructed by (5.1) are isomorphic if and only if they are of the same type.

We have verified Conjecture 6.5 computationally for $p \leq 5$. Taking advantage of Lemma 5.4, we can therefore conclude:

If $p = 2$, there is one isomorphism type of loops $Q(A)$ obtained from the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

of type 2. This is the unique commutative automorphic loop of order 8 that is not centrally nilpotent, constructed already in [10]. If $p = 3$, there are two isomorphism types of loops $Q(A)$, corresponding to

$$\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

of types 1 and 3, respectively. If $p = 5$, there are three isomorphism types. If Conjecture 6.5 is valid for a prime $p > 5$, then there are three isomorphism types of loops $Q(A)$ for that prime p, according to Lemma 5.4.

Acknowledgment. We are pleased to acknowledge the assistance of PROVER9 [15], an automated deduction tool, MACE4 [15], a finite model builder, and the GAP [5] package LOOPS [17]. PROVER9 was indispensable in the proofs of the lemmas leading up to Theorem 1.2. We used MACE4 to find the first automorphic loop of exponent 3 with trivial center in §5. We used the LOOPS package to verify Conjecture 6.5 for $p \leq 5$.

REFERENCES

[1] V. D. Belousov, *Foundations of the Theory of Quasigroups and Loops*, Izdat. Nauka, Moscow, 1967 (Russian).
[2] R. H. Bruck, *A Survey of Binary Systems*, Springer-Verlag, 1971.
[3] R. H. Bruck and L. J. Paige, Loops whose inner mappings are automorphisms, *Ann. of Math.* (2) **63** (1956), 308–323.
[4] D. A. S. de Barros, A. Grishkov and P. Vojtěchovský, Commutative automorphic loops of order p^3, in preparation.
[5] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.10*; 2007, (`http://www.gap-system.org`)
[6] G. Glauberman, On loops of odd order I, *J. Algebra* **1** (1964), 374–396.
[7] G. Glauberman, On loops of odd order II, *J. Algebra* **8** (1968), 393–414.
[8] G. Glauberman and C. R. B. Wright, Nilpotence of finite Moufang 2-loops. *J. Algebra* **8** (1968), 415–417.
[9] P. Jedlička, M. K. Kinyon and P. Vojtěchovský, The structure of commutative automorphic loops, *Trans. Amer. Math. Soc.* **363** (2011), 365–384.
[10] P. Jedlička, M. K. Kinyon and P. Vojtěchovský, Constructions of commutative automorphic loops, *Comm. Algebra*, to appear.
[11] K. W. Johnson, M. K. Kinyon, G. P. Nagy and P. Vojtěchovský, Searching for small simple automorphic loops, submitted.
[12] H. Kiechle, *The Theory of K-loops*, Lecture Notes in Math. **1778**, Springer-Verlag, Berlin, 2002.
[13] K. Kunen, M. K. Kinyon, J. D. Phillips and P. Vojtěchovský, The structure of automorphic loops, in preparation.
[14] M. Kinyon, J. D. Phillips and Vojtěchovský, When is the commutant of a Bol loop a subloop? *Trans. Amer. Math. Soc.* **360** (2008), no. 5, 2393–2408.
[15] W. McCune, *Prover9 and Mace4*, version 2009-11A, (`http://www.cs.unm.edu/~mccune/prover9/`)
[16] O. Perron, *Bemerkungen über die Verteilung der quadratischen Reste*, Mathematische Zeitschrift **56** (1952), no. **2**, 122–130.
[17] G. Nagy and P. Vojtěchovský, *LOOPS: Computing with quasigroups and loops in GAP* – a GAP package, version 2.0.0, 2008, (`http://www.math.du.edu/loops`)
[18] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math. **8**, Heldermann Verlag, Berlin, 1990.

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

(Kinyon and Vojtěchovský) Department of Mathematics, University of Denver, 2360 S Gaylord St, Denver, Colorado 80208 USA
E-mail address, Kinyon: mkinyon@math.du.edu
E-mail address, Vojtěchovský: petr@math.du.edu