# Nilpotency in automorphic loops of prime power order 

Přemysl Jedlička ${ }^{\text {a }, 1}$, Michael Kinyon ${ }^{\text {b }}$, Petr Vojtěchovský ${ }^{\text {b,* }}$<br>${ }^{\text {a }}$ Department of Mathematics, Faculty of Engineering, Czech University of Life Sciences, Kamýcká 129, 16521 Prague 6-Suchdol, Czech Republic<br>${ }^{\mathrm{b}}$ Department of Mathematics, University of Denver, 2360 S Gaylord St, Denver, CO 80208, USA

## A R T I C L E I N F O

## Article history:

Received 3 November 2010
Available online 16 November 2011
Communicated by Ronald Solomon

## MSC:

20N05

## Keywords:

Automorphic loop
Commutative automorphic loop
A-loop
Central nilpotency


#### 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 suitable elements of an anisotropic plane in the vector space of $2 \times 2$ matrices over the field of prime order $p$, we construct a family of automorphic loops of order $p^{3}$ with trivial center.


© 2011 Elsevier Inc. All rights reserved.

## 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 $[9,10]$.

[^0]We showed in [12, 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 [15], 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. [11], 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 [11, 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 [13].)

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.

### 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 $L_{x}: Q \rightarrow Q ; y \mapsto y L_{x}=x y$ and the right translation $R_{x}: Q \rightarrow Q ; y \mapsto y R_{x}=y x$ 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 Mlt $Q=\left\langle L_{X}, R_{x} \mid x \in Q\right\rangle$. The inner mapping group Inn $Q=(\text { Mlt } Q)_{1}$ is the stabilizer of $1 \in Q$. Standard references for the theory of loops are $[2,3,19]$.

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

The study of automorphic loops was initiated by Bruck and Paige [4]. 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 [11], as well as constructions and small order classification results [12].

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 $Z(Q)=F i x(\operatorname{Inn} Q)$, the set of fixed points of the inner mapping group. (See Section 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 $Z_{i+1}(Q), i \geqslant 0$, as the preimage of $Z\left(Q / Z_{i}(Q)\right)$ under the canonical projection. This defines the upper central series

$$
1 \leqslant Z_{1}(Q) \leqslant Z_{2}(Q) \leqslant \cdots \leqslant Z_{n}(Q) \leqslant \cdots \leqslant Q
$$

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 [11]. 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 o such that ( $Q, \circ$ ) is a Bruck loop (see Section 3), and such that powers of elements in ( $Q, \cdot$ ) coincide with those in $(Q, \circ)$.

Glauberman [8] 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 $n \geqslant 0$.

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

In Section 5, we use elements of anisotropic planes in the vector space of $2 \times 2$ matrices over $G F(p)$ 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 $p \geqslant 5$, and at least one (conjecturally, three) such loop for every prime $p \geqslant 7$.

Finally, we pose open problems in Section 6.

## 2. Preliminaries

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

- the left nucleus $\quad N_{\lambda}(Q)=\{a \in Q \mid a x \cdot y=a \cdot x y, \forall x, y \in Q\}$,
- the middle nucleus $\quad N_{\mu}(Q)=\{a \in Q \mid x a \cdot y=x \cdot a y, \forall x, y \in Q\}$,
- the right nucleus $\quad N_{\rho}(Q)=\{a \in Q \mid x y \cdot a=x \cdot y a, \forall x, y \in Q\}$,
- the nucleus $\quad N(Q)=N_{\lambda}(Q) \cap N_{\mu}(Q) \cap N_{\rho}(Q)$,
- the commutant $C(Q)=\{a \in Q \mid a x=x a, \forall x \in Q\}$,
- the center

$$
Z(Q)=N(Q) \cap C(Q)
$$

The commutant is not necessarily a subloop, but the nuclei are.
Proposition 2.1. (See [4].) In an automorphic loop ( $Q, \cdot), N_{\lambda}(Q)=N_{\rho}(Q) \leqslant N_{\mu}(Q)$. In a commutative automorphic loop $(Q, \cdot), Z(Q)=N_{\lambda}(Q)$.

We will also need the following (well known) characterization of $C(Q) \cap N_{\rho}(Q)$ :
Lemma 2.2. Let ( $Q$, .) be a loop. Then $a \in C(Q) \cap N_{\rho}(Q)$ if and only if $L_{a} L_{x}=L_{x} L_{a}$ for all $x \in Q$.
Proof. If $a \in C(Q) \cap N_{\rho}(Q)$, then for all $x, y \in Q, a \cdot x y=x y \cdot a=x \cdot y a=x \cdot a y$, that is, $L_{a} L_{x}=L_{x} L_{a}$. Conversely, if $L_{a} L_{x}=L_{x} L_{a}$ holds, then applying both sides to 1 gives $x a=a x$, i.e., $a \in C(Q)$, and then $x y \cdot a=a \cdot x y=x \cdot a y=x \cdot y a$, i.e., $a \in N_{\rho}(Q)$.

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

$$
L_{x, y}=L_{x} L_{y} L_{y x}^{-1}, \quad R_{x, y}=R_{x} R_{y} R_{x y}^{-1}, \quad T_{x}=R_{x} L_{x}^{-1}
$$

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

$$
(u v) L_{x, y}=u L_{x, y} \cdot v L_{x, y}
$$

for every $x, y, u, v$.
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 $\backslash: Q \times Q \rightarrow Q$ which satisfies

$$
x \backslash(x y)=x(x \backslash y)=y
$$

The division permutations $D_{\chi}: Q \rightarrow Q$ defined by $y D_{x}=y \backslash x$ are also quite useful, as is the inversion permutation $J: Q \rightarrow Q$ defined by $x J=x D_{1}=x^{-1}$ in any power-associative loop.

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

$$
\begin{align*}
x L_{y, x} & =x,  \tag{2.1}\\
L_{y, x} L_{x^{-1}} & =L_{x^{-1}} L_{y, x},  \tag{2.2}\\
y L_{y, x} & =((x y) \backslash x)^{-1},  \tag{2.3}\\
L_{x^{-1}, y^{-1}} & =L_{x, y},  \tag{2.4}\\
D_{x^{2}} & =D_{x} J D_{x}, \tag{2.5}
\end{align*}
$$

where the first two equalities follow from [11, Lem. 2.3], (2.3) from [11, Lem. 2.5], (2.4) is an immediate consequence of [11, Lem. 2.7], and (2.5) is [11, Lem. 2.8]. In addition, commutative automorphic loops satisfy the automorphic inverse property

$$
\begin{equation*}
(x y)^{-1}=x^{-1} y^{-1} \quad \text { and } \quad(x \backslash y)^{-1}=x^{-1} \backslash y^{-1}, \tag{2.6}
\end{equation*}
$$

by [11, Lem. 2.6].
Finally, as in [11], 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 [11, Lem. 2.3].
Lemma 2.3. For all $x, y$ in a commutative automorphic loop ( $Q, \cdot$ )

$$
\begin{align*}
\left(x^{-1}\right) P_{x y} & =x y^{2}  \tag{2.7}\\
x \cdot x P_{y} & =(x y)^{2} . \tag{2.8}
\end{align*}
$$

Proof. Eq. (2.7) is from [11, Lem. 3.2]. Replacing $x$ with $x^{-1}$ and $y$ with $x y$ in (2.7) yields $x P_{x^{-1} \cdot x y}=$ $x^{-1}(x y)^{2}$ and $x P_{x^{-1} \cdot x y}=x L_{x, x^{-1}} P_{x^{-1} \cdot x y}=x L_{x, x^{-1}} P_{y L_{x, x^{-1}}}$. Now, for every automorphism $\varphi$ of $Q$ we have $x \varphi P_{y \varphi}=(y \varphi)^{-1} \backslash(y \varphi x \varphi)=\left(y^{-1} \backslash(y x)\right) \varphi=x P_{y} \varphi$. Thus $x^{-1}(x y)^{2}=x L_{x, x^{-1}} P_{y L_{x, x^{-1}}}=x P_{y} L_{x, x^{-1}}$. 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

$$
\begin{equation*}
(x \circ(y \circ x)) \circ z=x \circ(y \circ(x \circ z)) . \tag{3.1}
\end{equation*}
$$

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

$$
x \circ y=\left[x^{-1} \backslash\left(x y^{2}\right)\right]^{1 / 2}=\left[\left(y^{2}\right) P_{x}\right]^{1 / 2}
$$

By [11, 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 $(Q, o)$ by $L_{x}^{\circ}$. For instance, we can express the fact that every Bol loop $(Q, o)$ is left power alternative by

$$
\begin{equation*}
\left(L_{x}^{\circ}\right)^{n}=L_{\chi^{n}}^{\circ} \tag{3.2}
\end{equation*}
$$

for all integers $n$.

Proposition 3.1. (See [14, 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 $x, y \in Q$,

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

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 $x \in Q$,

$$
\begin{equation*}
P_{a} P_{x}=P_{x} P_{a} \tag{3.3}
\end{equation*}
$$

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 $\left[\left(y^{2}\right) P_{x} P_{a}\right]^{1 / 2}=\left[\left(y^{2}\right) P_{a} P_{x}\right]^{1 / 2}$. 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 $x \in Q$,

$$
\begin{equation*}
x L_{a \backslash x, a}=x L_{a \backslash x^{-1}, a} \tag{4.1}
\end{equation*}
$$

Proof. First,

$$
\begin{aligned}
x^{-2} & =x^{-2} L_{a^{-1}}^{-1} L_{a^{-1}}=a^{-1} D_{x^{-2}} L_{a^{-1}} \\
& \stackrel{(2.6)}{=} a D_{x^{2}} J L_{a^{-1}} \stackrel{(2.5)}{=} a D_{x} J D_{x} J L_{a^{-1}} \\
& \stackrel{(2.6)}{=} a D_{x} D_{x^{-1}} L_{a^{-1}}=\left(x^{-1}\right) L_{a \backslash x}^{-1} L_{a^{-1}}
\end{aligned}
$$

Thus we compute

$$
\begin{align*}
\left(x^{-2}\right) L_{a \backslash x, a} & =\left(x^{-1}\right) L_{a \backslash x}^{-1} L_{a^{-1}} L_{a \backslash x, a} \stackrel{(2.2)}{=}\left(x^{-1}\right) L_{a \backslash x}^{-1} L_{a \backslash x, a} L_{a^{-1}} \\
& =\left(x^{-1}\right) L_{a} L_{x}^{-1} L_{a^{-1}}=a L_{x^{-1}} L_{x}^{-1} L_{a^{-1}} \\
& =a P_{x^{-1}} L_{a^{-1}} . \tag{4.2}
\end{align*}
$$

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

$$
\begin{aligned}
a P_{x^{-1}} L_{a^{-1}} & =a P_{x^{-1}} P_{a^{-1}} L_{a} \stackrel{(3.3)}{=} a P_{a^{-1}} P_{x^{-1}} L_{a} \\
& =a^{-1} P_{x^{-1}} L_{a} \stackrel{(4.2)}{=}\left(x^{-2}\right) L_{a^{-1} \backslash x, a^{-1}} \\
& \stackrel{(2.6)}{=}\left(x^{-2}\right) L_{\left(a \backslash x^{-1}\right)^{-1}, a^{-1}} \stackrel{(2.4)}{=}\left(x^{-2}\right) L_{a \backslash x^{-1}, a}
\end{aligned}
$$

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

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

$$
\begin{align*}
(a \backslash x) L_{a \backslash x^{-1}, a} & =(x \backslash a)^{-1},  \tag{4.3}\\
x^{-1} \cdot x P_{a} & =a^{2} . \tag{4.4}
\end{align*}
$$

Proof. We compute

$$
(a \backslash x) L_{a \backslash x^{-1}, a}=a \backslash\left(x L_{a \backslash x^{-1}, a}\right) \stackrel{(4.1)}{=} a \backslash\left(x L_{a \backslash x, a} \stackrel{(2.1)}{=}(a \backslash x) L_{a \backslash x, a} \stackrel{(2.3)}{=}(x \backslash a)^{-1},\right.
$$

where we used $L_{a \backslash x^{-1}, a} \in$ Aut $Q$ in the first equality and $L_{a \backslash x, a} \in$ Aut $Q$ in the third equality.
To show (4.4), we compute

$$
\begin{aligned}
x^{-1} \cdot x P_{a} & =\left(x^{-1}\right) L_{a^{-1} \backslash(a x)}=\left(x^{-1}\right) L_{a^{-1} \backslash(a x)} L_{a^{-1}} L_{a x}^{-1} L_{a x} L_{a^{-1}}^{-1} \\
& =(a \backslash(a x))^{-1} L_{a^{-1} \backslash(a x), a^{-1}} L_{a x} L_{a^{-1}}^{-1} \stackrel{(2.6)}{=}\left(a^{-1} \backslash(a x)^{-1}\right) L_{a^{-1} \backslash(a x), a^{-1}} L_{a x} L_{a^{-1}}^{-1} \\
& \stackrel{(4.3)}{=}\left((a x)^{-1} \backslash a^{-1}\right)^{-1} L_{a x} L_{a^{-1}}^{-1} \stackrel{(2.6)}{=}((a x) \backslash a) L_{a x} L_{a^{-1}}^{-1} \\
& =a L_{a^{-1}}^{-1}=a^{2} .
\end{aligned}
$$

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

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

$$
\begin{equation*}
L_{a}^{n}=L_{a^{n}} . \tag{4.5}
\end{equation*}
$$

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

$$
(a \circ x)^{2}=(x \circ a)^{2}=\left(a^{2}\right) P_{x} \stackrel{(4.4)}{=} x P_{a} L_{x^{-1}} P_{x}=x \cdot x P_{a} \stackrel{(2.8)}{=}(a x)^{2} .
$$

Taking square roots, we have $a \circ x=a x$, as desired. Then $L_{a}^{n}=\left(L_{a}^{\circ}\right)^{n} \stackrel{(3.2)}{=} L_{a^{n}}^{\circ}=L_{a^{n}}$.
Lemma 4.4. If $a \in Z(Q, \circ)$, then for all $x \in Q$,

$$
\begin{equation*}
P_{x a}=P_{x} P_{a} . \tag{4.6}
\end{equation*}
$$

Proof. For each $y \in Q$,

$$
y P_{x a}=y P_{a x}=\left[a x \circ y^{1 / 2}\right]^{2}=\left[(a \circ x) \circ y^{1 / 2}\right]^{2}=\left[a \circ\left(x \circ y^{1 / 2}\right)\right]^{2}=y P_{x} P_{a}
$$

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

$$
\begin{aligned}
L_{a^{2}} L_{x} & \stackrel{(4.5)}{=} L_{a}^{2} L_{x}=L_{a} L_{a, x} L_{x a} \\
& \stackrel{(2.4)}{=} L_{a} L_{a^{-1}, x^{-1}} L_{x a}=L_{a} L_{a^{-1}} L_{x^{-1}} L_{x^{-1} a^{-1}}^{-1} L_{x a} \\
& \stackrel{(4.5)}{=} L_{x^{-1}} L_{x^{-1} a^{-1}}^{-1} L_{x a} \stackrel{(2.6)}{=} L_{x^{-1}} L_{(x a)^{-1}}^{-1} L_{x a} \\
& =L_{x^{-1}} P_{x a} \stackrel{(4.6)}{=} L_{x^{-1}} P_{x} P_{a} \\
& =L_{x} L_{a} L_{a^{-1}}^{-1} \stackrel{(4.5)}{=} L_{x} L_{a}^{2} \\
& \stackrel{(4.5)}{=} L_{x} L_{a^{2}} .
\end{aligned}
$$

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 $Z(Q, \circ) \subseteq Z(Q, \cdot)$.

Proof. Assume that $a \in Z(Q, \circ)$. Then $a^{2} \in Z(Q, \cdot)$ by Lemma 4.5, and thus $\left(a L_{x, y}\right)^{2}=a^{2} L_{x, y}=a^{2}$ for every $x, y \in Q$. Taking square roots yields $a L_{x, y}=a$, 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 $Z\left(Q / Z_{n-1}(Q)\right)$ under the canonical projection, it follows by induction that it suffices to show $Z(Q, o)=Z(Q, \cdot)$. One inclusion is Lemma 4.6. For the other, suppose $a \in Z(Q, \cdot)$. Then $P_{a} P_{x}=L_{a} L_{a^{-1}}^{-1} L_{x} L_{x^{-1}}^{-1}=L_{x} L_{x^{-1}}^{-1} L_{a} L_{a^{-1}}^{-1}=P_{x} P_{a}$, 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 [8], ( $Q, \circ$ ) 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 [12] that for an odd prime $p$ a commutative automorphic loop of order $p, 2 p$, $4 p, p^{2}, 2 p^{2}$ or $4 p^{2}$ 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 [6], 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, we construct a family of automorphic loops of order $p^{3}$ with trivial nucleus.

### 5.1. Anisotropic planes

Let $F$ be a field, $V$ a finite-dimensional vector space over $F$, and $q: V \rightarrow F$ a quadratic form. A subspace $W \leqslant V$ is isotropic if $q(x)=0$ for some $0 \neq x \in W$, else it is anisotropic.

It is well known that if $F$ is a finite field and $\operatorname{dim} V \geqslant 3$ then $V$ must be isotropic. (See [21, Thm. 3.8] for a proof in odd characteristic.) Moreover, if $F=G F(p)$ then there is a unique anisotropic space of dimension 2 over $F$ up to isometry. (See [21, Cor. 3.10] for $p$ odd. If $p=2$ and $V=\langle x, y\rangle$, we must have $q(0)=0, q(x)=q(y)=q(x+y)=1$ for $V$ to be anisotropic.) Let us call anisotropic subspaces of dimension two anisotropic planes.

Since our construction is based on elements of anisotropic planes rather than on the planes themselves, we will first have a detailed look at anisotropic planes in $M(2, F)$, the vector space of $2 \times 2$ matrices over $F$. The determinant

$$
\operatorname{det}: M(2, F) \rightarrow F, \quad \operatorname{det}\left(\begin{array}{ll}
a_{1} & a_{2} \\
a_{3} & a_{4}
\end{array}\right)=a_{1} a_{4}-a_{2} a_{3}
$$

is a quadratic form on $M(2, F)$. If $F C \oplus F D$ is an anisotropic plane in $M(2, F)$ then $C^{-1}(F C \oplus F D)$ is also anisotropic, and hence, while looking for anisotropic planes, it suffices to consider subspaces $F I \oplus F A$, where $I$ is the identity matrix and $A \in G L(2, F)$.

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

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

We will now impose additional conditions on anisotropic planes over finite fields and establish their existence or non-existence. We will take advantage of the following strong result of Perron [17, Thms. 1 and 3] concerning additive properties of the set of quadratic residues.

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

Theorem 5.2 (Perron). Let $p$ be a prime, $N_{p}$ the set of quadratic nonresidues, and $R_{p}=\{a \in G F(p)$; $a$ is a quadratic residue or $a=0\}$.
(i) If $p=4 k-1$ and $a \neq 0$ then $\left|\left(R_{p}+a\right) \cap R_{p}\right|=k=\left|\left(R_{p}+a\right) \cap N_{p}\right|$.
(ii) If $p=4 k+1$ and $a \neq 0$ then $\left|\left(R_{p}+a\right) \cap R_{p}\right|=k+1,\left|\left(R_{p}+a\right) \cap N_{p}\right|=k$.

Lemma 5.3. Let $p \geqslant 5$ be a prime. Then there is a quadratic nonresidue a and quadratic residues $b, c$ such that $b-a$ is a quadratic residue and $c-a$ is a quadratic nonresidue.

Proof. Let $p=4 k \pm 1$. If $k \geqslant 3$ then we are done by Theorem 5.2, since $\left|\left(R_{p}-a\right) \cap R_{p}\right|$, $\left|\left(R_{p}-a\right) \cap N_{p}\right| \geqslant 3$. (We need $k \geqslant 3$ to be able to pick $b \in R_{p} \backslash\{0\}$ such that $b-a \in R_{p} \backslash\{0\}$.) If $p=7$ then $a=3, b=4, c=1$ do the job. If $p=5$ then $a=2, b=1, c=4$ do the job.

Lemma 5.4. Let $p$ be a prime and $F=G F(p)$.
(i) There is $A \in G L(2, p)$ such that $\operatorname{tr}(A)=0$ and $F I \oplus F A$ is anisotropic if and only if $p \neq 2$.
(ii) There is $A \in G L(2, p)$ such that $\operatorname{tr}(A) \neq 0, \operatorname{det}(A)$ is a quadratic residue modulo $p$ and $F I \oplus F A$ is anisotropic if and only if $p \neq 3$.
(iii) There is $A \in G L(2, p)$ such that $\operatorname{tr}(A) \neq 0, \operatorname{det}(A)$ is a quadratic nonresidue modulo $p$ and $F I \oplus F A$ is anisotropic if and only if $p \neq 2$.

Proof. Let $p \geqslant 3$. For a quadratic nonresidue $a$ and any $b \in F$, let

$$
M_{a, b}=\left(\begin{array}{cc}
-b & 1 \\
a & -b
\end{array}\right) .
$$

Since $M_{a, b}=M_{a, 0}-b I$, we have $F I \oplus F M_{a, b}=F I \oplus F M_{a, 0}$. $\operatorname{Now}, \operatorname{tr}\left(M_{a, 0}\right)=0, \operatorname{det}\left(M_{a, 0}-\lambda I\right)=\lambda^{2}-a$ has no roots, so $F I \oplus F M_{a, b}$ is anisotropic by Lemma 5.1. Moreover, if $b \neq 0$ then $\operatorname{tr}\left(M_{a, b}\right)=-2 b \neq 0$ and $\operatorname{det}\left(M_{a, b}\right)=b^{2}-a$.

If $p \geqslant 5$, Lemma 5.3 implies that the parameters $a$ and $b \neq 0$ can be chosen so that $\operatorname{det}\left(M_{a, b}\right)$ is a quadratic residue or nonresidue as we please.

Let $p=3$. Then $\operatorname{det}\left(M_{2,2}\right)$ is a quadratic nonresidue. If $\operatorname{tr}(A) \neq 0$ and $\operatorname{det}(A)$ is a quadratic residue then $\operatorname{det}(A)=1$ and $\operatorname{det}(A-\lambda I)$ is equal to either $\lambda^{2}+\lambda+1$ (with root 1 ) or $\lambda^{2}-\lambda+1$ (with root -1 ), so $F I \oplus F A$ is isotropic.

Let $p=2$. Then

$$
\left(\begin{array}{ll}
0 & 1 \\
1 & 1
\end{array}\right)
$$

satisfies the conditions of (ii). The only elements $A \in G L(2, p)$ with $\operatorname{tr}(A)=0$ are

$$
\left(\begin{array}{ll}
0 & 1 \\
1 & 0
\end{array}\right), \quad\left(\begin{array}{ll}
1 & 0 \\
1 & 1
\end{array}\right), \quad\left(\begin{array}{ll}
1 & 1 \\
0 & 1
\end{array}\right),
$$

all with $\operatorname{det}(A+I)=0$, so $F I \oplus F A$ is isotropic. There is no matrix satisfying the conditions of (iii) because there are no quadratic nonresidues in $G F(2)$.

Let $p$ be a prime and $F=G F(p)$. Call an element $A \in G L(2, p)$ of an anisotropic plane $F I \oplus F A$ of type 1 if $\operatorname{tr}(A)=0$, of type 2 if $\operatorname{tr}(A) \neq 0$ and $\operatorname{det}(A)$ is a quadratic residue, and of type 3 if $\operatorname{tr}(A) \neq 0$ and $\operatorname{det}(A)$ is a quadratic nonresidue.

Note that for a fixed prime $p$ we can find elements $A$ of all possible types (with the restrictions of Lemma 5.4) in a single anisotropic plane. This is because we only used matrices $A=M_{a, b}$ with the same $a$ in the proof of Lemma 5.4, and $F I \oplus F M_{a, 0}=F I \oplus F M_{a, b}$.
5.2. Automorphic loops of order $p^{3}$ with trivial nucleus

Let $A \in G L(2, p)$ be such that $F I \oplus F A$ is an anisotropic plane. Define a binary operation on $F \times$ ( $F \times F$ ) by

$$
\begin{equation*}
(a, x) \cdot(b, y)=(a+b, x(I+b A)+y(I-a A)) \tag{5.1}
\end{equation*}
$$

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

$$
U_{a}=I+a A
$$

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

$$
\begin{aligned}
& (b, y) L_{(a, x)}^{-1}=\left(b-a,\left(y-x U_{b-a}\right) U_{-a}^{-1}\right), \\
& (b, y) R_{(a, x)}^{-1}=\left(b-a,\left(y-x U_{a-b}\right) U_{a}^{-1}\right) .
\end{aligned}
$$

Lemma 5.5. Let $F=G F(p)$. Let $A \in G L(2, p)$ be such that $F I \oplus F A$ is an anisotropic plane in $M(2, p)$. For each $z \in F \times F$ and each $C \in G L(2, p)$ satisfying $C A=A C$, define $\varphi_{z, C}: F \times(F \times F) \rightarrow F \times(F \times F)$ by

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

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

$$
\begin{aligned}
(a, x) \varphi_{z, C} \cdot(b, y) \varphi_{z, C} & =(a, a z+x C) \cdot(b, b z+y C) \\
& =\left(a+b,(a z+x C) U_{b}+(b z+y C) U_{-a}\right) \\
& =\left(a+b,(a+b) z+x C U_{b}+y C U_{-a}+a b z A-a b z A\right) \\
& =\left(a+b,(a+b) z+\left(x U_{b}+y U_{-a}\right) C\right) \\
& =[(a, x) \cdot(b, y)] \varphi_{z, C}
\end{aligned}
$$

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

Proposition 5.6. Let $F=G F(p)$. Let $A \in G L(2, p)$ be such that $F I \oplus F A$ is an anisotropic plane in $M(2, p)$. Then the loop $Q=Q(A)$ defined on $F \times(F \times F)$ by (5.1) is an automorphic loop of order $p^{3}$ and exponent $p$ with $N_{\mu}(Q)=\{(0, x) \mid x \in F \times F\} \cong F \times F$ 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

$$
\begin{align*}
(b, y) T_{(a, x)} & =\left(b,\left(x\left(U_{-b}-U_{b}\right)+y U_{a}\right) U_{-a}^{-1}\right), \\
(c, z) R_{(a, x),(b, y)} & =\left(c,\left(z U_{a} U_{b}+y\left(U_{-c-a}-U_{-c} U_{-a}\right)\right) U_{a+b}^{-1}\right), \\
(c, z) L_{(a, x),(b, y)} & =\left(c,\left(z U_{-a} U_{-b}+y\left(U_{c+a}-U_{c} U_{a}\right)\right) U_{-a-b}^{-1}\right) . \tag{5.2}
\end{align*}
$$

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

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

Hence $Q(A)$ is automorphic by Lemma 5.5.
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 $(c, z) R_{(a, x),(b, y)}=(c, z)$ for every $(c, z),(b, y)$. Thus $\left(z U_{a} U_{b}+y\left(U_{-c-a}-U_{-c} U_{-a}\right)\right) U_{a+b}^{-1}=z$ for every $(c, z),(b, y)$. With $z=0$, we have $y\left(U_{-c-a}-U_{-c} U_{-a}\right)=-c a y A^{2}=0$ for every $y$, hence $c a A^{2}=0$ 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 $N_{\mu}(Q)=\{(0, x) \mid x \in F \times F\} \cong$ $F \times F$.

Suppose that $(c, z) \in N_{\lambda}(Q)$. By Proposition 2.1, $N_{\lambda}(Q)=N_{\rho}(Q) \leqslant N_{\mu}(Q)$, so $c=0$. We then must have $(0, z) R_{(a, x),(b, y)}=(0, z)$, or $z U_{a} U_{b} U_{a+b}^{-1}=z$, or $a b z A^{2}=0$ for every $a, b$. In particular, $z A^{2}=0$ and $z=0$. We have proved $N_{\lambda}(Q)=1$.

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 $x\left(U_{b}-U_{-b}\right)=y\left(U_{a}-U_{-a}\right)$, that is, $2 b x A=2 a y A$ for every $(b, y) \in Q$. With $b=0$ we deduce that $2 a y A=0$ for every $y$, thus $0=2 a A$, or $a=0$. Then $2 b x A=0$, and with $b=1$ we deduce $2 x A=0$, or $x=0$. We have proved that $C(Q)=1$.

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 $I+a A$ is invertible for every $a \in F$, which is a weaker condition than having $F I \oplus F A$ an anisotropic plane, as witnessed by $A=0$, for instance. But we claim that nothing of interest is obtained in the more general case:

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

$$
\begin{equation*}
z=\left(z U_{a} U_{b}+y\left(U_{-c-a}-U_{-c} U_{-a}\right)\right) U_{a+b}^{-1} \tag{5.3}
\end{equation*}
$$

for every $(a, x),(b, y)$. As $U_{b+a}-U_{b} U_{a}=-b a A^{2}=0$ for every $a, b$, we see that (5.3) holds.

## 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 $F=G F(p)$. Let $A, B \in G L(2, p)$ be such that $F I \oplus F A$ and $F I \oplus F B$ are anisotropic planes. Then the loops $Q(A), Q(B)$ constructed by (5.1) are isomorphic if and only if $A, B$ are of the same type.

We have verified Conjecture 6.5 computationally for $p \leqslant 5$. 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

$$
\left(\begin{array}{ll}
0 & 1 \\
1 & 1
\end{array}\right)
$$

of type 2 - this is the unique commutative automorphic loop of order 8 that is not centrally nilpotent, constructed already in [12]. If $p=3$, there are two isomorphism types of loops $Q(A)$, corresponding to matrices

$$
\left(\begin{array}{ll}
0 & 1 \\
2 & 0
\end{array}\right), \quad\left(\begin{array}{ll}
1 & 1 \\
2 & 1
\end{array}\right)
$$

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.

## Acknowledgments

After this paper was submitted for publication, P. Csörgő obtained a stronger result than Theorem 1.1 by her signature technique of connected group transversals. Namely, she proved:

Theorem 6.6 (Csörgő [5]). If $Q$ is a finite commutative automorphic $p$-loop ( $p$ an odd prime), then the multiplication group Mlt $Q$ is a p-group.

By a result of Albert [1], $Z($ Mlt $Q) \cong Z(Q)$. In particular, if Mlt $Q$ is a $p$-group then $Z(Q)$ is nontrivial. Our Theorem 1.1 then follows from Theorem 6.6 by an easy induction on the order of $Q$ (as observed by Csörgő in [5, Cor. 3.2]).

Actually, in hindsight it is not difficult to obtain Csörgő's Theorem 6.6 from our Theorem 1.1: In [22] (see also [20]), Shchukin proved that a commutative automorphic loop $Q$ is nilpotent of class at most $n$ if and only if Mlt $Q$ is nilpotent of class at most $2 n-1$. Now suppose $Q$ is a commutative automorphic $p$-loop, $p$ odd. By Theorem 1.1, $Q$ is nilpotent. By the result of Shchukin, Mlt $Q$ is nilpotent, hence a direct product of groups of prime power order. Since $Z(\mathrm{Mlt} Q) \cong Z(Q)$, it follows that $Z$ (Mlt $Q$ ) is a $p$-group. But then so is Mlt $Q$.

Finally, we are pleased to acknowledge the assistance of Proverg [16], an automated deduction tool, Mace4 [16], a finite model builder, and the GAP [7] package Loops [18]. Proverg 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 Section 5 . We used the Loops package to verify Conjecture 6.5 for $p \leqslant 5$.

## References

[1] A.A. Albert, Quasigroups, I, Trans. Amer. Math. Soc. 54 (1943) 507-519.
[2] V.D. Belousov, Foundations of the Theory of Quasigroups and Loops, Izdat. Nauka, Moscow, 1967 (in Russian).
[3] R.H. Bruck, A Survey of Binary Systems, Springer-Verlag, 1971.
[4] R.H. Bruck, L.J. Paige, Loops whose inner mappings are automorphisms, Ann. of Math. (2) 63 (1956) 308-323.
[5] P. Csörgö, Multiplication groups of commutative automorphic p-loops of odd order are p-groups, J. Algebra 350 (1) (2012) 77-83.
[6] D.A.S. de Barros, A. Grishkov, P. Vojtěchovský, Commutative automorphic loops of order $p^{3}$, submitted for publication.
[7] GAP Group, GAP - Groups, algorithms, and programming, version 4.4.10, 2007, http://www.gap-system.org.
[8] G. Glauberman, On loops of odd order I, J. Algebra 1 (1964) 374-396.
[9] G. Glauberman, On loops of odd order II, J. Algebra 8 (1968) 393-414.
[10] G. Glauberman, C.R.B. Wright, Nilpotence of finite Moufang 2-loops, J. Algebra 8 (1968) 415-417.
[11] P. Jedlička, M.K. Kinyon, P. Vojtěchovský, The structure of commutative automorphic loops, Trans. Amer. Math. Soc. 363 (2011) 365-384.
[12] P. Jedlička, M.K. Kinyon, P. Vojtěchovský, Constructions of commutative automorphic loops, Comm. Algebra 38 (9) (2010) 3243-3267.
[13] K.W. Johnson, M.K. Kinyon, G.P. Nagy, P. Vojtěchovský, Searching for small simple automorphic loops, London Math. Soc. J. Comput. Math. 14 (2011) 200-213.
[14] H. Kiechle, The Theory of $K$-Loops, Lecture Notes in Math., vol. 778, Springer-Verlag, Berlin, 2002.
[15] K. Kunen, M.K. Kinyon, J.D. Phillips, P. Vojtěchovský, The structure of automorphic loops, in preparation.
[16] W. McCune, Prover9 and Mace4, version 2009-11A, http://www.cs.unm.edu/~mccune/prover9/.
[17] O. Perron, Bemerkungen über die Verteilung der quadratischen Reste, Math. Z. 56 (2) (1952) 122-130.
[18] G. Nagy, P. Vojtěchovský, LOOPS: Computing with quasigroups and loops in GAP - a GAP package, version 2.0.0, 2008, http://www.math.du.edu/loops.
[19] H.O. Pflugfelder, Quasigroups and Loops: Introduction, Sigma Ser. in Pure Math., vol. 8, Heldermann-Verlag, Berlin, 1990.
[20] L.V. Safanova, K.K. Shchukin, On centrally nilpotent loops, Comment. Math. Univ. Carolin. 41 (2000) 401-404.
[21] W. Scharlau, Quadratic and Hermitian Forms, A Series of Comprehensive Stud. Math, vol. 270, Springer-Verlag, Berlin, 1985.
[22] K.K. Shchukin, On nilpotency of the multiplication group of an A-loop, Mat. Issled. 162 (1988) 116-117 (in Russian).


[^0]:    * Corresponding author.

    E-mail addresses: jedlickap@tf.czu.cz (P. Jedlička), mkinyon@math.du.edu (M. Kinyon), petr@math.du.edu (P. Vojtěchovský).
    ${ }^{1}$ Supported by the Grant Agency of the Czech Republic, grant No. 201/07/P015.

