On centerless commutative automorphic loops

Gábor P. Nagy

Abstract. In this short paper, we survey the results on commutative automorphic loops and give a new construction method. Using this method, we present new classes of commutative automorphic loops of exponent 2 with trivial center.

Keywords: commutative automorphic loop; Lie algebra of characteristic 2; nuclear extension

Classification: 20N05

1. Introduction

The set Q endowed with the binary operation $x \cdot y$ is a *quasigroup* if the equation $x \cdot y = z$ has a unique solution provided two of the variables x, y, z are known. The solution is denoted by $x = z/y$ and $y = x\backslash z$. The maps $R_y : x \mapsto x \cdot y$ and $L_x : y \mapsto x \cdot y$ are the *multiplication maps* of $(Q, \cdot)$; these are permutations of Q. The *multiplication group* $\mathrm{Mlt}(Q)$ is generated by the multiplication maps. Quasigroups with a unit element 1 are called *loops*; $L_1 = R_1 = \mathrm{id}$ holds. Let Q be a loop. The stabilizer subgroup of 1 in $\mathrm{Mlt}(Q)$ is the *group of inner mappings* $\mathrm{Inn}(Q)$. The loop Q is an *automorphic loop* if $\mathrm{Inn}(Q) \leq \mathrm{Aut}(Q)$. In particular, every group is an automorphic loop. The study of automorphic loops was initiated by Bruck and Paige [1] and it is in the very focus of recent research of the theory of loops and quasigroups.

Automorphic loops are power associative ([1]) and have the inverse property ([11]). Let Q be a finite automorphic loop. For any prime p, all elements of Q have p-power order iff $|Q|$ is a power of p ([12], [13]). We call such loops automorphic p-loops. Automorphic p-loops are solvable ([12], [13]). Automorphic loops of finite odd order are solvable ([13]). Automorphic loops of order p^2 are associative ([4], [13]). The class of finite commutative automorphic loops is interesting on its own. Most importantly, finite commutative automorphic loops are solvable ([12]). For an odd prime p, commutative automorphic p-loops are nilpotent ([3], [10]).

By now, there are many constructions showing that the above results are sharp in some sense. For any odd prime p, we have examples of nonnilpotent automorphic p-loops ([9], [10]). For any $n \geq 3$, there are examples of nonnilpotent commutative automorphic loops of order 2^n ([8]). If $p < q$ are primes and p divides $q-1$ or $q+1$, then we have examples of nonassociative commutative automorphic loops of order pq ([6]).

Finally, we mention that Lagrange and Cauchy Theorems are known to hold for commutative automorphic loops and automorphic loops of odd order. The main open problems in the theory of finite automorphic loops are the Sylow Theorems and the existence of nonassociative finite simple automorphic loops.

In this paper, we investigate finite commutative automorphic loops of exponent 2. Our main tool is the Lie ring method of [12], which was developed further in [13]. Our main result is to give a wide class of finite commutative automorphic loops of exponent 2 with trivial center.

2. Two constructions

In this section, we survey the properties of the two main construction methods of automorphic loops, namely the Lie ring method and the nuclear semidirect product method.

Let $(Q, +, [.,.])$ be a Lie ring and assume that

(W_1) for any $x \in Q$, the maps $y \mapsto y \pm [x, y]$ are invertible.

We define the operation

$$x \circ y = x + y - [x, y] \tag{1}$$

on Q. By [13, Lemma 5.1], $(Q, \circ)$ is a loop. The Lie ring ideals correspond to normal subloops, in particular, $[Q, Q]$ corresponds to the commutator-associator subloop of $(Q, \circ)$. Define the further properties of the Lie ring $(Q, +, [.,.])$:

(W_2) $[[x, y], [z, y]] = 0$ for all $x, y, z \in Q$.

(W_2^-) $(Q, \circ)$ is an automorphic loop.

(W_2^+) $[[x, y], [z, w]] = 0$ for all $x, y, z, w \in Q$.

Clearly, (W_2^+) implies (W_2). By [13, Proposition 5.2], (W_2) implies (W_2^-). The Lie ring $(Q, +, [.,.])$ is *uniquely* 2-*divisible* if the map $x \mapsto x + x$ is invertible. It was shown in [13, Lemma 5.8], that for uniquely 2-divisible Lie rings, (W_2^-) implies (W_2^+), that is, (W_2), (W_2^+) and (W_2^-) are equivalent. However, up to the author's knowledge, the situation is unknown in the general case. We formulate the problem for Lie rings of characteristic 2.

Problem 2.1. Let $(Q, +, [.,.])$ be a Lie ring of characteristic 2.

(a) Does (W_2^-) imply (W_2)?
(b) Does (W_2) imply (W_2^+)?

Notice that in this formulation of (b), no reference is made to property (W_1). In fact, we think that this question is interesting for general Lie rings of characteristic 2. Moreover, it is rather natural to restrict (b) to *nilpotent* Lie rings of characteristic 2; then (W_1) is automatically fulfilled. Using the Lie algebra database of the GAP package LieAlgDB [2], one can show that no nilpotent counterexample of dimension at most 9 exists, cf. Proposition A.1 in the appendix.

Another important observation is the following. If the answers to both questions (a) and (b) are affirmative, then any commutative automorphic loop of exponent 2, which is constructed from a Lie ring of characteristic 2 turns out to be associative modulo its middle nucleus. Indeed, by [13, Proposition 5.2], $a \in N_\mu(Q)$ iff $[[x,y],a]=0$ for all $x,y \in Q$. That is, (W_2^+) implies $[z,w] \in N_\mu(Q)$ for all $z,w \in Q$, and, the factor $Q/N_\mu(Q)$ is an elementary abelian 2-group. This fact justifies the importance of the class of commutative automorphic loops which are nuclear semidirect product of elementary abelian 2-groups. For the proofs of the following facts the reader is referred to [7].

Let H, K be abelian groups and $\Phi = \{\varphi_{i,j} \in \mathrm{Aut}(K) \mid i,j \in H\}$ a family of automorphisms such that

$$\varphi_{i,j} = \varphi_{j,i} \tag{2}$$

$$\varphi_{0,i} = \mathrm{id}_K \tag{3}$$

$$\varphi_{i,j} \circ \varphi_{k,n} = \varphi_{k,n} \circ \varphi_{i,j} \tag{4}$$

$$\varphi_{i,j+k} \circ \varphi_{j,k} = \varphi_{k,i+j} \circ \varphi_{i,j} \tag{5}$$

$$\varphi_{i,j+k} + \varphi_{j,i+k} + \varphi_{k,i+j} = \mathrm{id}_K + 2 \cdot \varphi_{i,j,k} \tag{6}$$

hold for all $i,j,k \in H$. Then, the underlying set $Q = K \times H$ endowed with the operation

$$(a,i) \star (b,j) = (\varphi_{i,j}(a+b), i+j) \tag{7}$$

is a commutative automorphic loop. Moreover, K is a normal subloop contained in the middle nucleus, $H \leq Q$, and $Q/K \cong H$. Conversely, if Q is an arbitrary commutative automorphic loop, K an abelian normal subloop contained in $N_\mu(Q)$, H an abelian subloop isomorphic to Q/K, then Q can be constructed by (7). It is worth mentioning that nonsplitting examples of order 32 can be constructed (see Proposition A.2 in the appendix). We remark further that if Q is a commutative automorphic loop of exponent 2 and $N_\mu(Q)$ has index 2 then Q splits.

Let H, K be elementary abelian 2-groups. [7, Proposition 1.4] implies that the center of Q is

$$\{(a,i) \mid \varphi_{j,k}(a) = a \ \text{ and } \ \varphi_{i,j} = \mathrm{id}_K \quad \text{for all} \quad j,k \in H\}.$$

In [8], the authors describe completely the case $|H| = 2$, that is, when the middle nucleus has index 2. In this case, Φ consists of id_K and a single nontrivial automorphism $\varphi = \varphi_{1,1}$. (In order to see this, use [8, Proposition 2.7] with the extra assumption that Q has exponent 2.) The construction of [8, Section 3.2] gives a commutative automorphic loop of exponent 2 with trivial center and order 2^n for any $n \geq 3$.

At the end of this section we make a closer look at the construction of [7, Theorem 4.3] and show that it has a nontrivial center. Let X be a subset of $\mathrm{End}(K)$ satisfying $X^2 = 0$. The group $G = \langle \mathrm{id}_K + x \mid x \in X \rangle_{\mathrm{Aut}(K)}$ is an elementary abelian 2-group and $\varphi : H^2 \to G$, $\varphi : (i,j) \mapsto \varphi_{i,j}$ a symmetric bilinear mapping. Since G has a common fixed point $a \in K$, the center of the resulting commutative automorphic loop is nontrivial.

3. Centerless commutative automorphic loops

For vector spaces K, H, we identify the subspaces $K \oplus 0$ and $0 \oplus H$ of $K \oplus H$ with K and H, respectively.

Lemma 3.1. *Let H, K be vector spaces over $\mathbb{F}_2$, and $\beta : H \to \mathrm{End}(K)$ a linear map. Define the bracket*

$$[a \oplus i, b \oplus j] = (\beta(j)a + \beta(i)b) \oplus 0 \tag{8}$$

on $Q = K \oplus H$. Then $(Q, +, [.,.])$ is a Lie algebra over $\mathbb{F}_2$ if and only if $\beta(i)$, $\beta(j)$ commute for all $i, j \in H$. Moreover, $[Q,Q] \subseteq K$ and $[[Q,Q],[Q,Q]] = 0$ hold.

Proof: The nontrivial part of the proof is the Jacobi identity which is equivalent to $\beta(i)\beta(j) + \beta(j)\beta(i) = 0$ by a straightforward calculation. □

Proposition 3.2. *Let H, K be vector spaces over $\mathbb{F}_2$, and $\beta : H \to \mathrm{End}(K)$ a linear map. Define the operation*

$$(a \oplus i) * (b \oplus j) = (a + b + \beta(j)a + \beta(i)b) \oplus (i + j) \tag{9}$$

on $Q = K \oplus H$. Assume that for all $i, j \in H$

(i) *the endomorphisms $\beta(i)$, $\beta(j)$ commute,*
(ii) *and $\mathrm{id} + \beta(i)$ is invertible.*

Then $(Q, *, 0)$ is a commutative automorphic loop of exponent 2 with the following properties:

(a) *$K \cap Z(Q) = \{a \in K \mid \beta(j)a = 0$ for all $j \in H\}$;*
(b) *$H \cap Z(Q) = \{i \in H \mid \beta(i)\beta(j) = 0$ for all $j \in H\}$;*
(c) *$Z(Q) = (K \cap Z(Q)) \oplus (H \cap Z(Q))$.*

In particular, if β is injective and at least one $\beta(j)$ is invertible then Q has trivial center.

Proof: Since the $\beta(i)$'s commute, $(Q, +, [.,.])$ is a Lie algebra with $[[Q,Q],[Q,Q]] = 0$ by Lemma 3.1. For fixed a, b, b', i, j, j',

$$\mathrm{id} + \mathrm{ad}_{a \oplus i} : b \oplus j \mapsto b' \oplus j'$$

holds iff $j = j'$ and $(\mathrm{id} + \beta(i))b = b' + \beta(j')a$. That is, $\mathrm{id} + \mathrm{ad}_{a \oplus i}$ is invertible iff $\mathrm{id} + \beta(i)$ is invertible. This means that $(Q, +, [.,.])$ satisfies (W_1) and $(Q, *, 0)$ is a commutative automorphic loop of exponent 2 by [13, Proposition 5.2]. We intend to show the properties of $Z(Q)$ by referring to [7, Proposition 1.4]. In order to do that, we must construct $(Q,*)$ as nuclear semidirect product. Put

$$\varphi_{i,j} = (\mathrm{id} + \beta(i+j))^{-1}(\mathrm{id} + \beta(i))(\mathrm{id} + \beta(j))$$

and

$$u(a \oplus i) = (\mathrm{id} + \beta(i))a \oplus i.$$

Then, using (9) and $\beta(i)\beta(j) = \beta(j)\beta(i)$

$$\begin{aligned} u(a \oplus i) * u(b \oplus j) &= ((\mathrm{id} + \beta(i))a \oplus i) * ((\mathrm{id} + \beta(j))b \oplus j) \\ &= [(\mathrm{id} + \beta(i))(\mathrm{id} + \beta(j))(a+b)] \oplus (i+j) \\ &= u(\varphi_{i,j}(a+b) \oplus (i+j)). \end{aligned}$$

Comparing this with (7), we see that u is an isomorphism between $(Q,*)$ and the nuclear semidirect product $(Q,\star)$, associated to $\Phi = \{\varphi_{i,j} \mid i,j \in H\}$. Now, [7, Proposition 1.4] implies (a), (b) and (c), since $\varphi_{i,j} = \mathrm{id}$ iff $\beta(i)\beta(j) = 0$. The last claim follows easily. $\square$

We finish the paper with two explicit examples of maps $\beta : H \to \mathrm{End}(K)$ which give rise to commutative automorphic loops of exponent 2 with trivial nucleus.

Example 1. Let K be a field of characteristic 2 and $\delta : H \hookrightarrow (K,+)$ an injective homomorphism such that $1 \notin \mathrm{Im}(\delta)$. Define $\beta : H \to \mathrm{End}_{\mathbb{F}_2}(K)$ by

$$\beta(i)(a) = \delta(i)a.$$

Then, β is injective and $\mathrm{id} + \beta(i)$ is invertible for all $i \in H$.

The next example is a special case of Example 1.

Example 2. Let K be a field of characteristic 2, H a proper subfield and $\sigma \in K \setminus H$. Define $\beta : H \to \mathrm{End}_{\mathbb{F}_2}(K)$ by

$$\beta(i)(a) = \sigma i a.$$

Then, β is injective and $\mathrm{id} + \beta(i)$ is invertible for all $i \in H$.

Appendix A. Low dimensional nilpotent Lie algebras

The Lie algebra database of the GAP package LieAlgDB [2] contains the complete list of nilpotent Lie algebras with dimension at most 9 over $\mathbb{F}_2$. We used this package for an exhaustive search for low dimensional counterexamples of Problem 2.1.

Proposition A.1 (Computational result). *Let $(Q,[.,.])$ be a nilpotent Lie algebra over $\mathbb{F}_2$ with $\dim Q \leq 9$. Then Q satisfies either all or none of (W_2), (W_2^+) and (W_2^-).*

Proof: The basic idea is to test Q first for (W_2). If (W_2) holds, then we test for (W_2^+), in the negative case Q would be a counterexample to (b). If (W_2) does not hold, then we test for (W_2^-), which would yield counterexample to (a) in the positive case. One can accelerate the test with the following tricks.

(i) Let B be a basis of Q over $\mathbb{F}_2$. (W_2) holds iff

$$[[x,y],[z,y]] = [[x,y],[z,w]] = 0$$

for all $x, y, z, w \in B$.

(ii) (W_2^+) holds iff the length of the Lie derived series of Q is at most 3.

(iii) Construct the loop $(Q, \circ)$ by (1). Let R be the right section of $(Q, \circ)$ and let S be a generating set of $\mathrm{Inn}(Q, \circ)$. Then, (W_2^-) holds iff $R = s^{-1}Rs$ for all $s \in S$. □

Since the number of nilpotent Lie algebras of dimension 5 over $\mathbb{F}_2$ is 9, the following example can be found.

Proposition A.2 (Computational result). *There exists a nilpotent Lie algebra $(Q, [.,.])$ of dimension 5 over $\mathbb{F}_2$ such that the corresponding loop $(Q, \circ)$ satisfies the following:*

(i) *$(Q, \circ)$ is a commutative automorphic loop of exponent 2;*

(ii) *the index of the middle nucleus is 4;*

(iii) *Q does not split nuclearly, that is, there are no subgroups H, K such that K is normal in Q, $K \le N_\mu(Q)$, $Q = HK$ and $H \cap K = \{1\}$.* □

Acknowledgment. The author would like to thank the referee for many valuable remarks, and Michael Kinyon (Denver) for a motivating discussion on low dimensional Lie algebras. The publication is supported by the European Union and co-funded by the European Social Fund. Project title: *Telemedicine-focused research activities on the field of Mathematics, Informatics and Medical Sciences*. Project number: TAMOP-4.2.2.A-11/1/KONV-2012-0073.

References

[1] Bruck R.H., Paige J.L., *Loops whose inner mappings are automorphisms*, Ann. of Math. (2) **63** (1956), 308–323.

[2] Cicalò S., de Graaf W.A., Schneider C., LieAlgDB – a GAP package, Version 2.1, November 2010, `http://www.gap-system.org/Packages/liealgdb.html`.

[3] Csörgő P., *The multiplication group of a finite commutative automorphic loop of order of power of an odd prime p is a p-group*, J. Algebra **350** (2012), 77–83.

[4] Csörgő P., *All automorphic loops of order p^2 for some prime p are associative*, J. Algebra Appl. **12** (2013), no. 6, 1350013.

[5] de Barros D.A.S., Grishkov A., Vojtěchovský P., *Commutative automorphic loops of order p^3*, J. Algebra Appl. **11** (2012), 1250100.

[6] Drápal A., *A class of commutative loops with metacyclic inner mapping groups*, Comment. Math. Univ. Carolin. **49** (2008), no. 3, 357–382.

[7] Hora J., Jedlička P., *Nuclear semidirect product of commutative automorphic loops*, J. Algebra Appl. **13** (2014), 1350077.

[8] Jedlička P., Kinyon M., Vojtěchovský P., *Constructions of commutative automorphic loops*, Comm. Algebra **38** (2010), no. 9, 3243–3267.
[9] Jedlička P., Kinyon M., Vojtěchovský P., *The structure of commutative automorphic loops*, Trans. Amer. Math. Soc. **363** (2011), no. 1, 365–384.
[10] Jedlička P., Kinyon M., Vojtěchovský P., *Nilpotency in automorphic loops of prime power order*, J. Algebra **350** (2012), 64–76.
[11] Johnson K.W., Kinyon M.K., Nagy G.P., Vojtěchovský P., *Searching for small simple automorphic loops*, LMS J. Comput. Math. **14** (2011), 200–213.
[12] Kinyon M., Grishkov A., Nagy G.P., *Solvability of commutative automorphic loops*, Trans. Amer. Math. Soc., to appear, `arXiv:1111.7138`.
[13] Kinyon M., Kunen K., Phillips J.D., Vojtěchovský P., *The structure of automorphic loops*, in preparation, `arXiv:1210.1642`.

Bolyai Institute, University of Szeged, Aradi vértanúk tere 1,
H-6720 Szeged, Hungary
and
MTA-ELTE Geometric and Algebraic Combinatorics Research Group,
Pázmány P. sétány 1/c, H-1117 Budapest, Hungary

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

(*Received* November 8, 2013)