Quasigroups and Related Systems **23** (2015), 237 − 242

Semidirect extensions of the Klein group leading to automorphic loops of exponent 2

Přemysl Jedlička

Abstract. In this paper we study automorphic loops of exponent 2 which are semidirect products of the Klein group with an elementary abelian group. It turns out that they fall into two classes: extensions of index 2 and extension using a symmetric bilinear form.

1. Introduction

A loop is called *automorphic* if all inner mappings are automorphisms. An automorphic loop of exponent 2 is always commutative due to the anti-automorphic inverse property [7]. There are several papers dealing with the structure of commutative automorphic loops, e.g. [1], [4] or [6]. It turns out that the structure of commutative automorhic 2-loops differs much from the theory of commutative automorphic p-loops, for odd primes p, and it is less understood.

The structure of commutative automorhic 2-loops is based on the structure of automorphic loops of exponent 2. It is already known that they are solvable [2] and that they need not be nilpotent [5]. Some constructions of automorphic loops of exponent 2 appeared in [5] and [8].

In this paper we construct automorphic loops of exponent 2 via the nuclear semidirect product defined in [3]. More precisely, we describe all the automorphic loops of exponent 2 that are nuclear semidirect extensions of the Klein group by an elementary abelian 2-group.

Theorem 1.1. *Let Q be an automorphic loop of exponent 2, let $K \lhd Q$ be a 4-element subgroup of $N_\mu(Q)$ and let H be a subgroup of Q such that $KH = Q$ and $|K \cap H| = 1$. Then one of the following situations occurs:*

(*a*) *Q is a group;*

(*b*) *$[Q : N_\mu(Q)] = 2$ and we can use Proposition 2.2;*

(*c*) *Q is a semidirect product based on a symmetric bilinear form described in Proposition 2.3.*

2010 Mathematics Subject Classification: 20N05
Keywords: automorphic loop, semidirect product, middle nucleus, exponent 2

The paper is organized as follows: in Section 2 we present the notion of the nuclear semidirect product of automorphic loops and also two situations when the semidirect product gives a loop of exponent 2. In Section 3 we analyze the semidirect product in the case when the image of the auxiliary mapping is a three-element group. Finally, in Section 4 we focus on the case when the image is a subgroup of order 2.

2. Preliminaries

We start our paper by recalling the notion of the nuclear semidirect product defined in [3] and by presenting two constructions that yield loops of exponent 2. Unlike in most loop theory papers, we shall use the additive notation here rather than the multiplicative one; the reason is that subgroups of our loops will appear as additive groups of vector spaces.

A semidirect product is a configuration of subloops in a loop $(Q,+)$: we have $H<Q$ and $K\lhd Q$ such that $K+H=Q$ and $K\cap H=0$. In [3] an external point of view was given, assuming additionally that $K\leqslant N_\mu(Q)$ and K being an abelian group. Such loops can be constructed given a special mapping φ.

Proposition 2.1 ([3]). *Let H and K be abelian groups and let us have a mapping $\varphi: H^2\to \mathrm{Aut}(K)$. We define an operation $*$ on $Q=K\times H$ as follows:*

$$(a,i)*(b,j)=(\varphi_{i,j}(a+b),i+j)\,.$$

This loop is denoted by $K\rtimes_\varphi H$. Let us denote $\varphi_{i,j,k}=\varphi_{i,j+k}\circ\varphi_{j,k}$. Then Q is a commutative A-loop if and only if the following properties hold:

$$\varphi_{i,j}=\varphi_{j,i} \tag{1}$$

$$\varphi_{0,i}=\mathrm{id}_K \tag{2}$$

$$\varphi_{i,j}\circ\varphi_{k,n}=\varphi_{k,n}\circ\varphi_{i,j} \tag{3}$$

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

$$\varphi_{i,j+k}+\varphi_{j,i+k}+\varphi_{k,i+j}=\mathrm{id}_K+2\cdot\varphi_{i,j,k} \tag{5}$$

Moreover, $K\times 0$ is a normal subgroup of Q, $0\times H$ is a subgroup of Q and $(K\times 0)\cap(0\times H)=0\times 0$ and $(K\times 0)+(0\times H)=Q$.

Q is associative if and only if $\varphi_{i,j}=\mathrm{id}_K$, for all $i,j\in H$. The nuclei are $N_\mu(Q)=K\times\{i\in H;\ \forall j\in H:\ \varphi_{i,j}=\mathrm{id}_K\}$ and
$N_\lambda=\{a\in K;\ \forall j,k\in H:\ \varphi_{j,k}(a)=a\}\times\{i\in H;\ \forall j\in H:\ \varphi_{i,j}=\mathrm{id}_K\}$.

On the other hand, if Q is a commutative automorphic loop, $K\lhd Q$ is a subgroup of $N_\mu(Q)$ and H is a subgroup of Q such that $K+H=Q$ and $K\cap H=\{0\}$ then there exists $\varphi: H^2\to\mathrm{Aut}\,K$ such that $Q\cong K\rtimes_\varphi H$.

The conditions $(1)-(5)$ are not too transparent and therefore it is worthwhile to present some special cases which are easier to describe. The simplest such a situation is probably the middle nucleus of index 2 which was described already in [5], not using the notion of a semidirect product.

Proposition 2.2 ([5], [3], exponent 2 version)**.** *Let K be an elementary abelian 2-group and let H be a two-element group. Then a mapping $\varphi : H^2 \to \operatorname{Aut} K$ satisfies the conditions (1) – (5) if and only if φ satisfies (2).*

On the other hand, if an automorphic loop Q has exponent 2 and $[Q : N_\mu(Q)] = 2$ then there exists such a φ with $Q \cong K \rtimes_\varphi H$.

In this paper, we are interested in loops of exponent 2. Among several configurations described in [3], there is one more that yields loops of exponent two: when the mapping φ is a symmetric bilinear form.

Proposition 2.3 ([3], exponent p version)**.** *Let K and H be elementary abelian p groups and let $f \in \operatorname{Aut} K$ be an automorphism of order p. Let $\varphi : H^2 \to \langle f \rangle$ be a symmetric bilinear form. Then φ satisfies conditions (1) – (5).*

In the rest of the paper we analyze the mapping φ when K is the Klein group. It will eventually turn out that all the possible solutions of φ are already described in Propositions 2.2 and 2.3.

3. Order 3 case

The automorphism group of the Klein group has only two non-trivial commutative subgroups, up to conjugacy. Each case will be analyzed separately. In this section we shall suppose that some of $\varphi_{i,j}$ is an automorphism of order 3. All the results can be proved under more general conditions.

Lemma 3.1. *Let K, H be elementary abelian 2-groups and let $\varphi : H^2 \to \operatorname{Aut} K$ satisfy (1) – (5). Then, for all $i, j \in H$,*

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

$$\varphi_{i,i+j} = \varphi_{i,i} \circ \varphi_{i,j}^{-1} \tag{7}$$

$$\varphi_{i,j}^2 = \varphi_{i,i} \circ \varphi_{j,j} \circ \varphi_{i+j,i+j}^{-1} \tag{8}$$

Proof. (6) is obtained from (5) via $k = i + j$. Then (4) gives

$$\varphi_{i,i} \circ \mathrm{id}_K = \varphi_{i,i} \circ \varphi_{0,j} = \varphi_{i,i,j} = \varphi_{i,j} \circ \varphi_{i,i+j}$$

which is (7). Finally (4) again gives

$$\varphi_{i+j,i+j} \circ \varphi_{i,j} = \varphi_{i,j,i+j} = \varphi_{i,i+j} \circ \varphi_{j,j}$$

and substituting (7) yields (8). □

If an automorphism of order 3 is contained within $\operatorname{Im} \varphi$, it turns out that the whole mapping φ is determined by its behavior on the planes of H.

Lemma 3.2. *Let K, H be elementary abelian 2-groups and let $\varphi : H^2 \to \operatorname{Aut} K$ satisfy $(1)-(5)$. Let $\operatorname{Im}\varphi \subseteq \{\mathrm{id}_K, f, f^2\}$, for some $f \in \operatorname{Aut} K$ with $f^3 = \mathrm{id}_K$, $f \neq \mathrm{id}_K$. Then, for all $i, j \in H$,*

(*i*) $|\{\alpha \in \{\varphi_{i,i}, \varphi_{j,j}, \varphi_{i+j,i+j}\};\ \alpha = f\}| \in \{0, 2\}$;

(*ii*) *there exists $k \in \langle i, j\rangle$ and $g \in \{\mathrm{id}_K, f, f^2\}$ such that, for all $v, w \in \langle i, j\rangle$,*

$$\varphi_{v,w} = \begin{cases} \mathrm{id}_K & \text{if } v \in \langle k\rangle \text{ or } w \in \langle k\rangle, \\ g & \text{if } v \notin \langle k\rangle \text{ and } w \notin \langle k\rangle. \end{cases}$$

Proof. (*i*) We find all the possible solutions of (6) within $\{\mathrm{id}_K, f, f^2\}$. They are, up to reordering, $(\mathrm{id}_K, \mathrm{id}_K, \mathrm{id}_K)$, (id_K, f, f) and $(\mathrm{id}_K, f^2, f^2)$.

(*ii*) We know from (*i*) all the possible choices of $\varphi_{i,i}$, $\varphi_{j,j}$ and $\varphi_{i+j,i+j}$. We put g to be that automorphism that appears at least twice within $\varphi_{i,i}$, $\varphi_{j,j}$ and $\varphi_{i+j,i+j}$ and we choose $k \in \{i, j, i+j\}$ such that $\varphi_{k,k} = \mathrm{id}_K$.

Then (8) gives

$$\varphi_{k,u}^2 = \varphi_{k,k} \circ \varphi_{u,u} \circ \varphi_{k+u,k+u}^{-1} = \mathrm{id}_K,$$

for each $u \in \langle i, j\rangle$, since $\varphi_{u,u} = \varphi_{k+u,k+u} = g$ and hence $\varphi_{k,u} = \mathrm{id}_K$. On the other hand, if $u, v \notin \langle k\rangle$ then

$$\varphi_{u,v}^2 = \varphi_{u,u} \circ \varphi_{v,v} \circ \varphi_{u+v,u+v}^{-1} = g^2,$$

for each $u \in \langle i, j\rangle$, since $u + v \in \langle k\rangle$ and therefore $\varphi_{u,v} = g$. □

Proposition 3.3. *Let K, H be elementary abelian 2-groups and let $\varphi : H^2 \to \operatorname{Aut} K$ satisfy $(1)-(5)$. Let $\operatorname{Im}\varphi \subseteq \{\mathrm{id}_K, f, f^2\}$, for some $f \in \operatorname{Aut} K$ with $f^3 = \mathrm{id}_K$. Then*

(*i*) *$\varphi_{i,j} \neq \mathrm{id}_K$ if and only if $\varphi_{i,i} = \varphi_{j,j} \neq \mathrm{id}_K$ and then $\varphi_{i,j} = \varphi_{i,i}$;*

(*ii*) $|\operatorname{Im}\varphi| < 3$;

(*iii*) *the set $M = \{k;\ \varphi_{k,k} = \mathrm{id}_K\}$ is a subspace of H of Co-dimension at most 1;*

(*iv*) *the middle nucleus of $K \rtimes_\varphi H$ is a subloop of index at most 2.*

Proof. For (*i*) we can restrict our focus to the subspace of dimension 2 and this was solved in Lemma 3.2.

(*ii*) Suppose $\varphi_{i,j} = f$ and $\varphi_{k,m} = f^2$. Due to (*i*) we can suppose $j = i$ and $m = k$. But this situation contradicts Lemma 3.2 (*ii*).

(*iii*) The set M is closed on addition due to Lemma 3.2 (*ii*). Moreover, every 2-dimensional subspace of H intersects M non-trivially and hence M is a hyperplane or $M = H$.

(*iv*) According to to Proposition 2.1, we have $N_\mu(K \rtimes_\varphi H) = K \times M$. □

4. Involutory case

In this section we analyze the second case, namely some $\varphi_{i,j}$ being an involution. Most lemmas can be pronounced in a more general setting again.

Lemma 4.1. *Let K, H be elementary abelian 2-groups and let $\varphi : H^2 \to \operatorname{Aut} K$ satisfy (1) – (5). Moreover, let $\varphi_{i,j}^2 = \mathrm{id}_K$, for each $i, j \in H$. Then*

$$\varphi_{i,j} + \varphi_{i,k} + \varphi_{j,k} = \varphi_{i,j,k} \tag{9}$$

$$\varphi_{i,j+k} = (\varphi_{i,j} + \varphi_{i,k} + \varphi_{j,k}) \circ \varphi_{j,k} \tag{10}$$

for all $i, j, k \in H$.

Proof. When we multiply (5) by $\varphi_{i,j,k}$, we obtain

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

which is (9) since $\varphi_{i,j,k} \circ \varphi_{i,j+k} = \varphi_{j,k}$ due to (4). And plugging (9) into (4), namely $\varphi_{i,j+k} = \varphi_{i,j,k} \circ \varphi_{j,k}$, gives (10). □

Corollary 4.2. *Let K and H be elementary abelian 2-groups and let B be a basis of H. Suppose that we have a mapping $\varphi' : B^2 \to \operatorname{Aut} K$ such that $(\varphi'_{i,j})^2 = \mathrm{id}_K$, for each $i, j \in B$. Then there exists at most one mapping $\varphi : H^2 \to \operatorname{Aut} K$, satisfying (1) – (5) such that $\varphi_{i,j}^2 = \mathrm{id}_K$, for each $i, j \in H$, and $\varphi|_{B^2} = \varphi'$.*

Proof. By an induction using (10). □

Corollary 4.2 claims that φ is uniquely determined whenever we know its values on a basis. It need not exist though, e.g. conditions (1) or (3) may be violated already by φ'. But it exists if φ' is a symmetric matrix with two different entries.

Proposition 4.3. *Let K and H be two elementary abelian 2-groups and let $\varphi : H^2 \to \operatorname{Aut} K$ satisfy (1) – (5). Suppose that $\operatorname{Im} \varphi = \{\mathrm{id}_K, f\}$, for some involutory $f \in \operatorname{Aut} K$. Then φ is a bilinear mapping.*

Proof. Let us take a basis B of the space H. The restriction $\varphi|_{B^2}$ is symmetric and hence induces a symmetric bilinear form, let us say φ', from H^2 to $\{\mathrm{id}_K, f\} \cong \mathbb{Z}_2$. According to Proposition 2.3, the mapping φ' satisfies the conditions (1) – (5). Since $\varphi'|_{B^2} = \varphi|_{B^2}$, Corollary 4.2 gives $\varphi = \varphi'$. □

We are now ready to prove Theorem 1.1.

Proof of Theorem 1.1. Conditions of Proposition 2.1 are met and hence there exists a mapping $\varphi : H^2 \to \operatorname{Aut} K$ satisfying (1)–(5).

If $\varphi_{i,j}$ is an involution, for some $i, j \in H$, then $|\operatorname{Im} \varphi| = 2$, due to (1), since involutions in $\operatorname{Aut} \mathbb{Z}_2^2$ commute only with themselves and with the identity. Then Proposition 4.3 gives that φ is bilinear.

On the other hand, if no involution appears in $\operatorname{Im} \varphi$ then $\operatorname{Im} \varphi \subseteq \{\mathrm{id}_K, f, f^2\}$, where f and f^2 are the automorphisms of order 3. And Proposition 3.3 states that the middle nucleus is a subgroup of index at most 2. □

What if K is a larger elementary abelian group? There are three more types of subgroups even in $\operatorname{Aut} \mathbb{Z}_2^3$ and therefore it is likely that some new construction type will be needed.

References

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

[2] **A. Grishkov, M.K. Kinyon, G.P. Nagy**, *Solvability of commutative automorphic loops*, Proceedings AMS **142** (2014), 3029 – 3037.

[3] **J. Hora, P. Jedlička**, *Nuclear semidirect product of commutative automorphic loops*, J. Algebra Appl. **13** (2014), no.1, paper 1350077.

[4] **P. Jedlička, M. Kinyon, P. Vojtěchovský**, *Structure of commutative automorphic loops*, Trans. AMS **363** (2011), 365384.

[5] **P. Jedlička, M. Kinyon, P. Vojtěchovský**, *Constructions of commutative automorphic loops*, Commun. Algebra **38** (2010), 3243 – 3267.

[6] **P. Jedlička, M. Kinyon, P. Vojtěchovský**, *Nilpotency in automorphic loops of prime power order*, J. Algebra **350** (2012), 64 – 76.

[7] **K.W. Johnson, M.K. Kinyon, G.P. Nagy, P. Vojtěchovský**, *Searching for small simple automorphic loops*, LMS J. Comput. Math. **14** (2011), 200 – 213.

[8] **G.P. Nagy**, *On centerless commutative automorphic loops*, Comment. Math. Univ. Carol. **55** (2014), 485 – 491.

Received October 14, 2014

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