# NUCLEAR SEMIDIRECT PRODUCT OF COMMUTATIVE AUTOMORPHIC LOOPS

JAN HORA AND PŘEMYSL JEDLIČKA

Abstract. Automorphic loops are loops where all inner mappings are automorphisms. We study when a semidirect product of two abelian groups yields a commutative automorphic loop such that the normal subgroup lies in the middle nucleus. With this description at hand we give some examples of such semidirect products.

A *loop* is a quasigroup with a neutral element, that means an algebra $(Q, \cdot, 1)$ satisfying $1 \cdot x = x \cdot 1 = x$ and the mappings $L_a : x \mapsto a \cdot x$ and $R_a : x \mapsto x \cdot a$ being bijective. The *multiplication group* $\mathrm{Mlt}(Q)$ is the permutation group on $Q$ generated by all the $L_a$ and $R_a$. The *inner mapping group* $\mathrm{Inn}(Q)$ is the stabiliser of 1 within $\mathrm{Mlt}(Q)$. A loop is called *automorphic* (or an A-loop) if $\mathrm{Inn}(Q) \subseteq \mathrm{Aut}(Q)$. A subset of $Q$ is called a *subloop* if it is closed on the binary operation and if it is a loop. A subloop $S$ of $Q$ is called *normal* if every inner mapping of $Q$ sends $S$ to $S$.

The commutative automorphic loops have been studied intensively in recent years [5] and a few examples were constructed too [6], [3]. Some of these examples are in fact semidirect products and this brought the idea, how the semidirect product of commutative A-loops look like.

The answer in the full generality is probably difficult, given how complicated already the semidirect product of Moufang loops is [4]. This is why focus on a special case, called the nuclear semidirect product. The *middle nucleus* of a loop $Q$ is $N_\mu(Q) = \{x \in Q;\ a(xb) = (ax)b,\ \forall a, b \in Q\}$. Here we consider only those semidirect products $Q = K \rtimes H$, satisfying $K \subseteq N_\mu(Q)$ and $H$ abelian.

The semidirect product can be viewed as two different notions—on one hand, it is a special configuration of subalgebras in an algebra and on the other hand it is a construction giving a larger object from two smaller ones. In section 1 we start with a given configuration (that means $K \triangleleft Q$, $H < Q$, $K \cap H = \{1\}$ and $KH = Q$) and we deduce how can it be described externally, that means using some mapping $\varphi : H^2 \to \mathrm{Aut}(K)$.

In Section 2 we give some examples that were already known before, only the fact of being semidirect products was not emphasised. In Section 3 we study what loops can be obtained if the normal subgroup is cyclic with less than 5 elements; a construction found there is subsequently generalized for larger subgroups. In Section 4 we study the situation from Section 3 in deeper details giving a more general description.

As a byproduct, we show that, for each prime $p$, all but two commutative A-loops of order $p^3$ can be obtained as semidirect products and we give their descriptions.

*Date*: October 29, 2012, *Version*: 0.81 $\gamma$.

## 1. Analysis of the semidirect product

In this section we give a description of the semidirect product we want to understand. Let us first recall what a semidirect product of groups is. There is an internal semidirect product, that means a configuration of two subgroups, $K \triangleleft G$ and $H < G$ such that $KH = G$ and $K \cap H = \{1\}$. On the other hand, external semidirect product is a construction $(K \rtimes_\varphi H, *)$ on the set $K \times H$ given by the law $(a, i) * (b, j) = (a\varphi_j(b), ij)$, for some $\varphi : H \mapsto \mathrm{Aut}(K)$.

In the loop case, a loop $Q$ is a semidirect product, if we find two subloops $K$ and $H$ of $Q$ such that $K$ is normal and $K \cap H = \{1\}$ and $K \cdot H = Q$. However, as we said before, the description in the full generality is complicated and this is why we decided to restrain the area of our interest and focus on the case where

- $K$ and $H$ are abelian groups,
- $K \leqslant N_\mu(Q)$.

To see that this restriction is not general, see the next example.

**Example 1.1.** There exists only one non-associative commutative Moufang loop on 81 elements. Denote it by $Q$. It is well-known [9] that all commutative Moufang loops are automorphic. There exists a normal subgroup, let us say $K$, of $Q$ with 27 elements. Since $Q$ is of exponent 3, the loop $Q$ is a semidirect product of $K$ and $\langle x \rangle$, for any $x \notin K$. Nevertheless $K \not\subseteq N_\mu(Q)$ as the nucleus contains only 3 elements. This calculation can be easily verified using GAP [8].

From now on, we will be dealing with an internal semidirect product, i.e., we consider the following situation: we have a commutative automorphic loop $Q$ with two subgroups $K$ and $H$, where $K \triangleleft Q$ and $K \leqslant N_\mu(Q)$. Both groups are abelian and, in the sequel, they will often serve as additive groups of rings. This is why we shall use the additive notation rather than the multiplicative one. Hence, the conditions of the semidirect product are written as $K \cap H = \{0\}$ and $K + H = Q$.

When working with quasigroups, there are usually two parastrophic operations defined: $a/b$ as the solution of the equation $ax = b$ and $a\backslash b$ as the solution of the equation $xa = b$. Here we consider commutative quasigroups with the additive notation and therefore it is natural to denote the (one) associated operation by $-$.

**Lemma 1.2.** *For each element $x$ of $Q$, there exists a unique expression $x = a + i$, for $a \in K$ and $i \in H$.*

*Proof.* Existence follows from $K + H = Q$. Suppose now $a + i = b + j$. Then $i = (j + b) - a = j + (b - a)$ since $b \in N_\mu(Q)$. This implies $(b - a) \in H$ and $a = b$. The rest follows. □

This lemma did not need the assumption of automorphicity. This will definitely not be the case of other statements and hence we have to recall some basic properties of commutative A-loops from [2]. The inner mapping group of a commutative loop is generated by mappings

$$R_{x,y} = R_{x+y}^{-1} \circ R_x \circ R_y.$$

The left nucleus of a loop is the set $N_\lambda(Q) = \{x \in Q;\ x+(y+z) = (x+y)+z,\ \forall y, z \in Q\}$. In general there is no connection between the left and the middle nucleus but in the case of commutative loops, the inclusion $N_\lambda(Q) \subseteq N_\mu(Q)$ was proved in [2].

Turning back to the semidirect product: a semidirect product of groups is described by a mapping $\varphi : H \to \mathrm{Aut}(K)$ and, in fact, each automorphism from $\mathrm{Im}\,\varphi$

is a restriction of an inner automorphism of $K \rtimes_\varphi H$, that means of a mapping $k \mapsto h^{-1}kh$. In the case of commutative automorphic loops, inner automorphisms come into play too.

**Lemma 1.3.** *Let $i, j \in H$. Then there exists an automorphism $\varphi_{i,j} \in \mathrm{Aut}(K)$ such that, for all $a, b \in K$,*

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

*Proof.* Let us denote $q_{a,b} = ((a + i) + (b + j)) - (i + j)$. Since $a$ and $b$ lie in the middle nucleus, we have

$$\begin{aligned}(a + i) + (b + j) = ((a + i) + b) + j = ((i + a) + b) + j \\ = (i + (a + b)) + j = ((a + b) + i) + j.\end{aligned}$$

Hence we have $q_{a,b} = (((a + b) + i) + j) - (i + j) = R_{i+j}^{-1} R_j R_i(a + b) = R_{i,j}(a + b)$. Since $R_{i,j}$ is an inner mapping, it sends $K$ onto $K$. Since $Q$ is automorphic, $R_{i,j}$ has to be an automorphism of $K$. □

Unlike for groups, here the generators of the inner automorphism group are the mappings $R_{x,y}$ and this is why we need two parameters for the mapping $\varphi$.

**Proposition 1.4.** *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:*

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

*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 $N_\lambda = \{a \in K;\ \forall j, k \in H :\ \varphi_{j,k}(a) = a\} \times \{i \in H;\ \forall j \in H :\ \varphi_{i,j} = \mathrm{id}_K\}$.*

*Proof.* "⇒" Properties (1) and (2) encode a commutative loop. The other three should encode a right automorphic loop. Let us denote by $(a, i)/(b, j)$ the solution of the equation $(a, i) * (x, y) = (b, j)$. We see that

$$(a, i)/(b, j) = (\varphi_{i-j,j}^{-1}(a) - b, i - j)$$

Then we calculate the inner mapping. We already use (1) implicitly.

$$\begin{aligned}[(u, m) * [(v, n) * (a, i)]/[(u, m) * (v, n)] = \\ [(u, m) * (\varphi_{n,i}(v + a), n + i)]/[(u, m) * (v, n)] \\ = \big(\varphi_{m,n+i}(u + \varphi_{n,i}(v + a)), m + n + i\big)/(\varphi_{m,n}(u + v), m + n) \\ = \big(\varphi_{m+n,i}^{-1}\varphi_{m,n+i}(u + \varphi_{n,i}(v + a)) - \varphi_{m,n}(u + v), i\big)\end{aligned}$$

We want the inner mapping to be a homomorphism and hence we compare

$$(6)\quad [(u,m)*[(v,n)*[(a,i)*(b,j)]]]/[(u,m)*(v,n)] = \\ \big(\varphi^{-1}_{m+n,i+j}\varphi_{m,n+i+j}(u+\varphi_{n,i+j}(v+\varphi_{i,j}(a+b)))-\varphi_{m,n}(u+v), i+j\big)$$

and

$$(7)\quad [(u,m)*[(v,n)*(a,i)]]/[(u,m)*(v,n)]* \\ [(u,m)*[(v,n)*(b,j)]]/[(u,m)*(v,n)] = \big(\varphi_{i,j}\big(\varphi^{-1}_{m+n,i}\varphi_{m,n+i}(u+ \\ \varphi_{n,i}(v+a))+\varphi^{-1}_{m+n,j}\varphi_{m,n+j}(u+\varphi_{n,j}(v+b))-2\varphi_{m,n}(u+v)\big), i+j\big)$$

A commutative loop is automorphic if and only if all inner mappings are homomorphisms, i.e., if (6)=(7). Setting $b=u=v=0$ and $i=0$ we obtain

$$(8)\qquad \varphi^{-1}_{m+n,j}\varphi_{m,n+j}\varphi_{n,j}(a)=\varphi_{m,n}(a)$$

which is actually a slightly different version of (4). Now, setting $b=u=v=0$ in (6) and using (8) we obtain

$$\varphi^{-1}_{m+n,i+j}\varphi_{m,n+i+j}\varphi_{n,i+j}\varphi_{i,j}(a)=\varphi_{m,n}\varphi_{i,j}(a)$$

and in (7) we get

$$\varphi_{i,j}\varphi^{-1}_{m+n,i}\varphi_{m,n+i}\varphi_{n,i}(a)=\varphi_{i,j}\varphi_{m,n}(a).$$

Hence the automorphisms commute and we proved (3). Moreover, combining (8) and (3) we prove (4). Finally we set $a=b=v=0$ in (6) obtaining

$$\varphi^{-1}_{m+n,i+j}\varphi_{m,n+i+j}(u)-\varphi_{m,n}(u)=\varphi_{m,n}\varphi^{-1}_{n,i+j}(u)-\varphi_{m,n}(u)=\varphi_{m,n}(\varphi^{-1}_{n,i+j}(u)-u)$$

and then in (7) to get

$$\varphi_{i,j}(\varphi^{-1}_{m+n,i}\varphi_{m,n+i}(u)+\varphi^{-1}_{m+n,j}\varphi_{m,n+j}(u)-2\varphi_{m,n}(u))= \\ \varphi_{i,j}(\varphi_{m,n}\varphi^{-1}_{n,i}(u)+\varphi_{m,n}\varphi^{-1}_{n,j}(u)-2\varphi_{m,n}(u))=\varphi_{m,n}\varphi_{i,j}(\varphi^{-1}_{n,i}(u)+\varphi^{-1}_{n,j}(u)-2u).$$

Thus we have by cancelling $\varphi_{m,n}$

$$\begin{aligned}\varphi^{-1}_{n,i+j}(u)-u&=\varphi_{i,j}(\varphi^{-1}_{n,i}(u)+\varphi^{-1}_{n,j}(u)-2u)\\ \varphi_{n,i+j}(\varphi^{-1}_{n,i+j}(u)+\varphi_{i,j}(2u))&=\varphi_{n,i+j}(\varphi_{i,j}(\varphi^{-1}_{n,i}(u)+\varphi^{-1}_{n,j}(u))+u)\\ u+\varphi_{n,i,j}(2u)&=\varphi_{n,i,j}\varphi^{-1}_{n,i}(u)+\varphi_{n,i,j}\varphi^{-1}_{n,j}(u)+\varphi_{n,i+j}(u)\\ u+2\varphi_{n,i,j}(u)&=\varphi_{n+i,j}(u)+\varphi_{n+j,i}(u)+\varphi_{n,i+j}(u)\end{aligned}$$

and this is the last of the necessary conditions, namely (5).

"⇐" In order to prove that the conditions are sufficient, we simplify both expressions of the left inner mapping. The first coordinate of the left hand side simplifies to

$$\varphi_{m,n}\varphi^{-1}_{n,i+j}(u+\varphi_{n,i+j}(v+\varphi_{i,j}(a+b)))-\varphi_{m,n}(u+v) \\ =\varphi_{m,n}(\varphi^{-1}_{n,i+j}(u)-u)+\varphi_{m,n}\varphi_{i,j}(a+b)$$

while the other side is

$$\varphi_{i,j}(\varphi_{m,n}\varphi^{-1}_{n,i}(u+\varphi_{n,i}(v+a)+\varphi_{m,n}\varphi^{-1}_{n,j}(u+\varphi_{n,j}(v+b)-2\varphi_{m,n}(u+v) \\ =\varphi_{m,n}(\varphi_{i,j}(\varphi^{-1}_{n,i}(u)+v+a+\varphi^{-1}_{n,j}(u)+v+b-2u-2v) \\ =\varphi_{m,n}\varphi_{i,j}(\varphi^{-1}_{n,i}(u)+\varphi^{-1}_{n,j}(u)-2u+a+b)$$

and both sides are equal if $\varphi_{n,i+j}^{-1}(u) - u = \varphi_{i,j}(\varphi_{n,i}^{-1}(u) + \varphi_{n,j}^{-1}(u) - 2u)$. However, this is equivalent to (5) as we proved in the previous paragraph.

Now we compute the middle nucleus.

$$((a,i) * (b,j)) * (c,k) =$$
$$(\varphi_{i+j,k}(\varphi_{i,j}(a+b)+c), i+j+k) = (\varphi_{i,j,k}(a+b+\varphi_{i,j}^{-1}(c)), i+j+k),$$
$$(a,i) * ((b,j) * (c,k)) =$$
$$(\varphi_{i,j+k}(a+\varphi_{j,k}(b+c)), i+j+k) = (\varphi_{i,j,k}(\varphi_{j,k}^{-1}(a)+b+c)), i+j+k).$$

Since $\varphi_{i,j,k}$ is an automorphism, both the expressions are equal if and only if $a + \varphi_{i,j}^{-1}(c) = \varphi_{j,k}^{-1}(a) + c$. An element $(b,j)$ lies in the middle nucleus if and only if the equality holds for all elements, in particular for $c = 0$. This yields $\varphi_{j,k}(a) = a$, for all $a \in K$ and $k \in H$. The same argument gives that $(a,i) \in N_\lambda(Q)$ if and only if $\varphi_{i,j} = \mathrm{id}_K$ and $\varphi_{j,k}(a) = a$, for all $j,k \in H$. □

## 2. Known examples

In this section we recapitulate the already known constructions of commutative A-loops that are nuclear semidirect products.

Suppose $|H| = 2$ first. All commutative A-loops with the middle nucleus of index 2 were analysed in [6] hence we cannot discover anything new here. Nevertheless, this case is very simple and therefore we show how such semidirect products look like.

If $H = \mathbb{Z}_2$ then the semidirect product is described by the automorphism $\varphi_{1,1}$ since the others are trivial by (2). Properties (1), (3) and (4) are then fulfilled trivially and the non-trivial one is (5). More precisely, the only choice that is not automatically satisfied is

$$3 \cdot \mathrm{id}_K = 3 \cdot \varphi_{1,0} = \mathrm{id}_K + 2 \cdot \varphi_{1,1,1} = \mathrm{id}_K + 2\varphi_{1,1} \circ \varphi_{1,0} = \mathrm{id}_K + 2\varphi_{1,1}.$$

From this we obtain $2a = 2\varphi_{1,1}(a) = \varphi_{1,1}(2a)$, for each $a \in K$. On the other hand, it was proved in [6] that choosing any automorphism of $K$ that satisfies $\varphi_{1,1}(2a) = 2a$ yields a commutative automorphic loop and two different constructions are isomorphic if and only if the chosen automorphisms are similar.

Another semidirect product was presented in [7], based on a more complicated construction by Drápal [3]. Using the properties (1)–(5) it is easier now to show that the loop so constructed is a commutative A-loop and we can even generalize the construction a little bit.

**Proposition 2.1.** *Let $M$ be a faithful module over a ring $R$, $\mathrm{char}(R) \neq 2$, and let $r \in R^*$ be of a multiplicative order $k \in \mathbb{N} \cup \{\infty\}$. Suppose that $(r^i + 1) \in R^*$, for each $i \in \mathbb{Z}$. Then the set $M \times \mathbb{Z}_k$ equipped with the operation*

$$(a,i) * (b,j) = \left( \frac{(r^i+1)\cdot(r^j+1)}{2\cdot(r^{i+j}+1)} \cdot (a+b),\ i+j \right)$$

*is a commutative A-loop.*

*Proof.* We prove that the construction is a semidirect product given by the mapping $\varphi_{i,j} : x \mapsto \frac{(r^i+1)\cdot(r^j+1)}{2\cdot(r^{i+j}+1)} \cdot x$. Indeed, a multiplication by an invertible ring element is an automorphism of $M$. From now on we will not be making a distinction between an element of $R$ and its multiplication endomorphism.

When we prove properties (1)–(5), we shall know that the semidirect product yields a commutative A-loop. The ring itself is not commutative in general but the subring of $R$ generated by $r$ is commutative and hence we have (1). Properties (2) and (3) are evident. For (4) we compute $\varphi_{i,j,k} = \frac{(r^i+1)\cdot(r^j+1)\cdot(r^k+1)}{4\cdot(r^{i+j+k}+1)}$ and this does not depend on the ordering of the elements.

Property (5) has to be computed manually. The left hand side is

$$\frac{(r^i+1)\cdot(r^{j+k}+1)}{2\cdot(r^{i+j+k}+1)} + \frac{(r^j+1)\cdot(r^{i+k}+1)}{2\cdot(r^{i+j+k}+1)} + \frac{(r^k+1)\cdot(r^{i+j}+1)}{2\cdot(r^{i+j+k}+1)} = \frac{3+r^i+r^j+r^k+r^{i+j}+r^{i+k}+r^{j+k}+3\cdot r^{i+j+k}}{2\cdot(r^{i+j+k}+1)}$$

while the right hand side is

$$1+2\cdot\frac{(r^i+1)\cdot(r^j+1)\cdot(r^k+1)}{4\cdot(r^{i+j+k}+1)} = \frac{2(r^{i+j+k}+1)+(r^i+1)(r^j+1)(r^k+1)}{2\cdot(r^{i+j+k}+1)} = \frac{2r^{i+j+k}+2+1+r^i+r^j+r^k+r^{i+j}+r^{i+k}+r^{j+k}+r^{i+j+k}}{2\cdot(r^{i+j+k}+1)}$$

Both sides are equal, which proves (5). □

This construction was presented in [7] for $R$ a field. To justify the generalisation, we need to bring an example where $R$ is not a field.

**Corollary 2.2.** *Let $V$ be a vector space over a field $F$, char $F \neq 2$, $\dim V = n$. Let $A$ be a regular matrix of size $n$, satisfying $A^k = I$, for some odd $k$. Then the set $V \times \mathbb{Z}_k$ equipped with the operation*

$$(\vec{u}, i) * (\vec{v}, j) = \left(\tfrac{1}{2}\cdot(\vec{u}+\vec{v})\cdot(A^i+I)\cdot(A^j+I)\cdot(A^{i+j}+I)^{-1},\ i+j\right)$$

*is a commutative A-loop.*

*Proof.* The vector space is a faithful module over the ring of matrices and hence the only thing to prove is that $(A^i+I)$ is regular, for each $i$. Suppose, by contradiction, that $(A^i+I)$ is singular. Then $-1$ is an eigenvalue of $A^i$. Hence there exists $\lambda$, an eigenvalue of $A$ in the closure field $\overline{F}$, such that $\lambda^i = -1$. But we know that $A^k = I$ and hence $\lambda^k = 1$ which is a contradiction since $k$ is odd. □

**Example 2.3.** Let $F$ be a field of an odd characteristic $p$. Let $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. Then $A^p = I$ and we obtain a commutative A-loop on the set $F^3 \times \mathbb{Z}_p$. This loop is not associative because $\varphi_{1,1} = \begin{pmatrix} 1 & 0 & -1/4 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

## 3. Small cyclic normal subgroup

In this section we study how the semidirect product looks if the normal subgroup is small, that means less than five elements, and cyclic. We still keep the notation from Section 1 and we add one more—since $\mathrm{End}(K) \cong K$, for $K$ cyclic, we shall not distinguish the elements of $K$ and the elements of $\mathrm{End}(K)$. It will be clear from the context whether we work with an element $a$ of $K$ itself or with the mapping $x \mapsto a \cdot x$. It turns out that the only small interesting cyclic case is the group $\mathbb{Z}_4$.

**Proposition 3.1.** *If $|K| \leq 3$ then $Q$ is associative.*

*Proof.* If $|K| < 3$ then there exists only one automorphism of $K$. Suppose hence $|K| = 3$.

We analyse Property (5). First we put $i = j$ and $k = -i$ and we obtain $\varphi_{2i,-i} + 2\varphi_{0,i} = 1 + 2\varphi_{i,i,-i}$ and therefore $\varphi_{2i,-i} = 2\varphi_{i,i,-i} - 1$. Since 0 is not an automorphism, this equation has only one solution: $\varphi_{i,i,-i} = \varphi_{2i,-i} = 1$. Moreover, $1 = \varphi_{i,i,-i} = \varphi_{2i,-i} \circ \varphi_{i,i} = \varphi_{i,i}$.

Now we put $k = i$. This yields $\varphi_{i,i,j} = \varphi_{2i,j} \circ \varphi_{i,i}$ and hence $\varphi_{i,i,j} = \varphi_{2i,j}$. Finally, from $\varphi_{2i,j} + 2\varphi_{i,i+j} = 1 + 2\varphi_{i,i,j}$ we cancel the same automorphisms, obtaining $2\varphi_{i,i+j} = 1 + \varphi_{i,i,j}$. Once again, this equation has only one solution, namely $\varphi_{i,i+j} = 1$, for all $i, j \in H$. Hence $Q$ is associative. □

We shall focus on the case $K \cong \mathbb{Z}_4$. The automorphisms of $\mathbb{Z}_4$ are the multiplication by 1 and the multiplication by 3. We study the conditions under which these two mappings satisfy Property (5). It turns out that many things can be proved in a broader generality, like the following lemma.

**Lemma 3.2.** *Let $m, n \in \mathbb{N}$. Let $a \equiv b \equiv c \equiv 1 \pmod{mn}$. Then $ab + bc + ca \equiv 1 + 2abc \pmod{mn^2}$. In particular, if $a$, $b$ and $c$ are odd then $a + b + c \equiv abc + 2 \pmod 4$.*

*Proof.* We write $a = a'mn + 1$, $b = b'mn + 1$ and $c = c'mn + 1$. Then

$$\begin{aligned} ab + bc + ca &= a'b'm^2n^2 + a'mn + b'mn + 1 + b'c'm^2n^2 + b'mn + c'mn + 1 \\ &\qquad + a'c'm^2n^2 + a'mn + c'mn + 1 \\ &\equiv 2(a' + b' + c')mn + 3 \pmod{mn^2} \\ 1 + 2abc &= 1 + 2\big(a'b'c'm^3n^3 + a'b'm^2n^2 + b'c'm^2n^2 + a'c'm^2n^2 \\ &\qquad + a'mn + b'mn + c'mn + 1\big) \\ &\equiv 2(a' + b' + c')mn + 3 \pmod{mn^2} \end{aligned}$$

In particular, if $m = 1$, $n = 2$ and $a, b, c$ are odd then $ab+bc+ca \equiv 1+2abc \pmod 4$. We then multiply both sides of the equivalence by $abc$ and obtain $c+a+b \equiv abc+2 \pmod 4$ since odd squares are congruent to 1 modulo 4. □

**Lemma 3.3.** *If $K \cong \mathbb{Z}_4$ then $\varphi_{i+j,k} = \varphi_{i,k} \circ \varphi_{j,k}$.*

*Proof.* We analyse Property (5). Since both automorphisms are involutory, when multiplying both sides by $\varphi_{i,j,k}$, we obtain $\varphi_{i,j} + \varphi_{i,k} + \varphi_{j,k} = \varphi_{i,j,k} + 2$. Lemma 3.2 gives us $\varphi_{i,j} + \varphi_{i,k} + \varphi_{j,k} = \varphi_{i,j}\varphi_{j,k}\varphi_{k,i} + 2$. Therefore we get $\varphi_{i,j,k} = \varphi_{i,j}\varphi_{i,k}\varphi_{j,k}$.

Now $\varphi_{i,j}\varphi_{i,k}\varphi_{j,k} = \varphi_{i,j,k} = \varphi_{i,j}\varphi_{i+j,k}$ and cancelling $\varphi_{i,j}$ we obtain the claim. □

If $K \cong \mathbb{Z}_4$, a necessary condition is $\varphi_{i+j,k} = \varphi_{i,k} \circ \varphi_{j,k}$, that means that $\varphi$ is a bilinear mapping. It turns out that the condition is sufficient too. Moreover, this result can be generalized for other cyclic groups. We recall that *radical* of a symmetric bilinear form $\alpha$ is the set $\operatorname{Rad}\alpha = \{x;\ \alpha(x, y) = 0,\ \forall y\}$.

**Proposition 3.4.** *Let $K = \mathbb{Z}_{mn^2}$, for some $m, n \in \mathbb{N}$. Let $H$ be an abelian group and let $\alpha : H^2 \to \mathbb{Z}_n$ be a symmetric bilinear form. We define $\varphi_{i,j} : x \mapsto (\alpha(i, j) \cdot mn + 1) \cdot x$. Then $K \rtimes_\varphi H$ is a commutative A-loop. Moreover $N_\mu(Q) = K \times \operatorname{Rad}\alpha$ and $N_\lambda(Q) \cong \operatorname{Ann}(mn \operatorname{Im}\alpha) \times \operatorname{Rad}\alpha$.*

*Proof.* We have to remark first that $(a \cdot mn + 1) \cdot (b \cdot mn + 1) \equiv ((a + b) \cdot mn + 1) \pmod{mn^2}$, for all $a, b \in \mathbb{Z}$, and hence $\varphi_{i+j,k} = (\alpha(i + j, k) \cdot mn + 1) = ((\alpha(i, k) + \alpha(j, k)) \cdot mn + 1) = \varphi_{i,k}\varphi_{j,k}$.

Now, properties (1)–(3) are clearly satisfied. Property (4) follows from $\varphi_{i,j,k} = \varphi_{i,j}\varphi_{i,k}\varphi_{j,k}$. Property (5) is then shown in Lemma 3.2.

Ad nuclei: $\varphi_{i,j} = 1$ for all $j \in H$ if and only of $\alpha(i, j) = 0$ for all $j \in H$. From this we get the middle nucleus. The left nucleus contains those $(a, i) \in N_\mu(Q)$, such that $(\alpha(j, k) \cdot mn + 1) \cdot a = a$ and hence $\alpha(j, k) \cdot mna{=}0$, for all $j, k \in H$. □

We assumed $\alpha$ to be arbitrary but it turns out that, in the case of vector spaces, only non-degenerate forms give interesting results.

**Lemma 3.5.** *Suppose all the assumptions of Proposition 3.4. Let $H = H_1 \times H_2$ such that $\alpha(H, H_2) = 0$. Then $K \rtimes_\varphi H \cong (K \rtimes_\varphi H_1) \times H_2$.*

*Proof.* The isomorphism $K \rtimes_\varphi H_1 \times H_2 \mapsto K \rtimes_\varphi H$ is $\gamma : (a, i, j) \mapsto (a, i + j)$. This mapping is clearly a bijection, we verify that it is a homomorphism.

$$\begin{aligned}
\gamma((a, i, j) * (b, k, l)) &= \gamma(((\alpha(i + k) + 1)mn(a + b), i + k, j + l)) \\
&= ((\alpha(i + k) + 1)mn(a + b), i + j + k + l)) \\
\gamma((a, i, j)) * \gamma((b, k, l)) &= (a, i + j) * (b, k + l) \\
&= ((\alpha(i + j, k + l)mn + 1)(a + b), i + j + k + l)
\end{aligned}$$

and both expressions are equal since $\alpha(i + j, k + l) = \alpha(i, k) + \alpha(i, l) + \alpha(j, k) + \alpha(j, l) = \alpha(i, k)$. □

A natural question is the isomorphism type of the loops so obtained. In the case of vector spaces, the answer is as expected.

**Proposition 3.6.** *Let $K = \mathbb{Z}_{mp^2}$, for some prime $p$, and let $H$ be an elementary abelian $p$-group. Let us have two bilinear forms $\alpha_1, \alpha_2 : H^2 \to \mathbb{Z}_p$. Let $Q_1$ and $Q_2$ be two loops obtained via the construction in Proposition 3.4, using the forms $\alpha_1$ resp. $\alpha_2$. Then $Q_1 \cong Q_2$ if and only if $\alpha_1$ and $\alpha_2$ are equivalent.*

*Proof.* "⇐" Let there exist $\beta$, an automorphism of $H$ such that $\alpha_2(\beta(i), \beta(j)) = \alpha_1(i, j)$, for all $i, j \in H$. Define $\gamma : Q_1 \to Q_2$, $(a, i) \mapsto (a, \beta(i))$. We claim that $\gamma$ is an isomorphism.

$$\begin{aligned}
\gamma((a, i) *_1 (b, j)) &= \gamma(((\alpha_1(i, j) \cdot mp + 1) \cdot (a + b), i + j)) \\
&= (((\alpha_1(i, j) \cdot mp + 1) \cdot (a + b), \beta(i + j))) \\
\gamma(a, i) *_2 \gamma(b, j) &= (a, \beta(i)) *_2 (b, \beta(j)) = ((\alpha_2(\beta(i), \beta(j))mp + 1)(a + b), \\
\beta(i) + \beta(j)) &= (((\alpha_1(i, j) \cdot mp + 1) \cdot (a + b), \beta(i + j)))
\end{aligned}$$

and $\gamma$ is a homomorphism. The bijection is clear.

"⇒" Let $\alpha_1$ and $\alpha_2$ be nonequivalent symmetric bilinear forms. If the dimensions of the radicals of the forms $\alpha_i$ are not equal, we get, by Proposition 3.4, different sizes of middle nuclei and thus non-isomorphic corresponding loops. Thus we can assume that the dimensions of the radicals of the forms $\alpha_i$ are equal. Moreover, by Lemma 3.5 the loop is then a direct product of the radical and of a smaller loop. We can hence suppose that $\alpha_1$ and $\alpha_2$ are non-degenerate.

Let $\gamma$ be an isomorphism $Q_1 \to Q_2$. Since $\alpha_1$ and $\alpha_2$ are non-degenerate, $N_\mu(Q_1) = N_\mu(Q_2) = K \times 0$. And therefore $\gamma$ restricted on $K \times 0$ is an automorphism (we shall thus understand $\gamma$ as an automorphism of $K$). On the other

hand $\gamma(H) \neq H$ in general. Let us write $\gamma((0,i)) = (\delta(i), \beta(i))$, for $i, \beta(i) \in H$ and $\delta(i) \in K$. We thus have $\gamma((a,i)) = (\gamma(a), 0) *_2 (\delta(i), \beta(i)) = (\gamma(a) + \delta(i), \beta(i))$. Now

$$\begin{aligned}\gamma((a,i) *_1 (b,j)) &= \gamma(((\alpha_1(i,j) \cdot mp + 1) \cdot (a+b), i+j)) \\ &= (\gamma(((\alpha_1(i,j) \cdot mp + 1) \cdot (a+b)) + \delta(i+j), \beta(i+j))) \\ \gamma(a,i) *_2 \gamma(b,j) &= (\gamma(a) + \delta(i), \beta(i)) *_2 (\gamma(b) + \delta(j), \beta(j)) \\ &= ((\alpha_2(\beta(i), \beta(j))mp + 1)((\gamma(a) + \delta(i)) + (\gamma(b) + \delta(j)))), \beta(i) + \beta(j))\end{aligned}$$

Since $\gamma$ is an automorphism, $\beta$ has to be an automorphism of $H$. Now, putting $a = b = 0$, we get

$$\delta(i+j) = (\alpha_2(\beta(i), \beta(j))mp + 1)(\delta(i) + \delta(j)) \qquad (\star)$$

Plugging $(\star)$ into the calculation, we obtain

$$\begin{aligned}\gamma(a,i) *_2 \gamma(b,j) &= ((\alpha_2(\beta(i), \beta(j))mp + 1)((\gamma(a) + \gamma(b)) + (\delta(i) + \delta(j)))), \beta(i+j)) \\ &= ((\alpha_2(\beta(i), \beta(j))mp + 1)(\gamma(a) + \gamma(b))) + \delta(i+j), \beta(i+j))\end{aligned}$$

from which

$$\gamma(((\alpha_1(i,j) \cdot mp + 1) \cdot (a+b) = (\alpha_2(\beta(i), \beta(j))mp + 1)(\gamma(a) + \gamma(b)).$$

Since all automorphisms of $\mathbb{Z}_{mp^2}$ commute, we obtain

$$\alpha_1(i,j) \cdot mp = \alpha_2(\beta(i), \beta(j)) \cdot mp$$

and the bilinear forms are equivalent. □

When we know equivalence classes, we can enumerate loops, up to isomorphism.

**Corollary 3.7.** *Let $K = \mathbb{Z}_{mp^2}$, for some prime $p$, and let $H \cong \mathbb{Z}_p^k$, for some $k \in \mathbb{N}$. The number of loops, up to isomorphism, that can be constructed by Proposition 3.4 is*

- $2k + 1$, *if $p$ is odd;*
- $\lfloor \frac{3}{2}k \rfloor + 1$, *if $p = 2$.*

*Proof.* It is well known that, if the characteristics of the vector space is different from 2, every symmetric bilinear form is equivalent to a diagonal form. For every nonzero dimension of $H$ there are up to equivalence precisely two non-degenerate symmetric forms. Possible representatives of the two classes are diagonal forms $(1, 1, \ldots, 1)$ and $(1, 1, \ldots, d)$, where $d$ is a non-square element of the field.

If the characteristic is 2 then there are two possibilities: a symmetric form is either equivalent to a diagonal form or an alternating one. There are $k + 1$ non-equivalent diagonal forms. A non-degenerate form exists on even dimensions only and is unique up to equivalence. If we count degenerate forms too, there are $\lfloor \frac{k}{2} \rfloor + 1$ alternating forms (including one trivial). □

*Remark* 3.8. The previous corollary did enumerate all possible commutative A-loops but did not give a hint how to distinguish them structurally, especially those coming from non-degenerate forms. If $p$ is odd and the dimension is $2k$, we get by Witt's theorem that the two non-equivalent forms differ in the dimension of (any) maximal isotropic subspace (usually called index or Witt index). One of the forms has index $k$ and the other $k-1$ and thus the size of any maximal associative subloop of $Q$ containing $K$ differ for the two loops obtained by the construction. On the other hand, if the dimension is odd, the two non-equivalent forms are similar (one is

a multiple of the other) and thus the structure of the corresponding loops is similar (see Example 3.9).

If $p = 2$ then the two loops obtained from the non-degenerate forms on even dimension can also be distinguished by their structure. Let $i$ be an element of $H$ and consider the subloop $S_i$ generated by the middle nucleus $N_\mu(Q) = K$ and an element $(a, i)$. Since the middle nucleus contains the element $(-a, 0)$, the definition of $S_i$ does not depend on $a$ and thus we can assume $a = 0$. If $\alpha$ is alternating then any $S_i$ is a group because $\alpha \equiv 0$ on the set $\langle i\rangle \times \langle i\rangle$. If $\alpha$ is not alternating then there exists $i \in H$ satisfying $\alpha(i, i) \neq \mathrm{id}_K$ and we get $S_i$ non-associative:

$$\begin{aligned}((1, i) * (0, i)) * (0, i) &= (\varphi_{i,i}(1), 0) * (0, i) = (\varphi_{i,i}(1), i),\\ (1, i) * ((0, i) * (0, i)) &= (1, i) * (0, 0) = (1, i)\end{aligned}$$

**Example 3.9.** All commutative A-loops of order $p^3$, for $p$ prime, were presented in [6]. It was then proved in [1] that they form exactly seven isomorphism classes. Two of them (respectively three, if $p = 3$) have their middle nucleus cyclic of order $p^2$. Both the loops, for $p \geqslant 5$, are structurally very similar and the articles did not explain how and why these two loops differ. Here we give a new point of view at these loops. They can be constructed using Proposition 3.4, with those two nonequivalent forms.

In the case of characteristic 2, there exists only one non-trivial bilinear form on dimension 1. The other loop of order 8, as well as the third loop of order 27, cannot be obtained as a semidirect product; they contain no element of order $p$ outside of the middle nucleus.

## 4. Bilinear mappings

In Section 3, we found examples of semidirect products where the mapping $\varphi$ is bilinear. In this section, we shall investigate this phenomenon further on, and find a general condition when $\varphi$ happens to be bilinear. In that case we have $\varphi_{i,j,k} = \varphi_{i,j}\varphi_{i,k}\varphi_{j,k}$ and Property (5) rewrites as

$$\varphi_{i,k}\varphi_{j,k} + \varphi_{j,i}\varphi_{j,k} + \varphi_{i,k}\varphi_{j,k} = \mathrm{id}_K + 2\varphi_{i,j}\varphi_{i,k}\varphi_{j,k}.$$

We start the section by investigating when could such a situation happen.

**Lemma 4.1.** *Let $R$ be a commutative ring. Let $G$ be a subgroup of $R^*$. Then the following properties are equivalent*

- *for all $a, b, c \in G$, we have $ab + bc + ca = 1 + 2abc$;*
- *for all $a, b, c \in G$, we have $a + b + c = abc + 2$;*
- *for all $a, b \in G$, we have $ab = a + b - 1$.*

*Proof.* (i)⇒(ii) We have $a^{-1}b^{-1} + b^{-1}c^{-1} + c^{-1}a^{-1} = 1 + 2a^{-1}b^{-1}c^{-1}$. Multiplying this equality by $abc$, we obtain $c + a + b = abc + 2$.

(ii)⇒(iii): $2 + ab = 2 + ab \cdot 1 = a + b + 1$.

(iii)⇒(i) $1 + 2abc = 1 + 2(a + b - 1)c = 1 + 2(ac + bc - c) = 1 + 2(a + c - 1 + b + c - 1 - c) = 2a + 2b + 2c - 3 = (a + b - 1) + (b + c - 1) + (c + a - 1) = ab + bc + ca$ □

**Lemma 4.2.** *Let $R$ be a unitary ring and let $n \in \mathbb{N}$. Then the following properties are equivalent:*

- *there exists a generating subset $\{x_1, \ldots, x_k\}$ of $R$ such that $nx_i = 0$ and $x_i x_j = 0$, for all $i, j$;*

- *$R$ is a commutative ring and there exists $G$, a subgroup of $R^*$ generating $R$, such that, for all $a, b, c \in G$, we have $na = n$ and $ab + bc + ca = 1 + 2abc$.*

*Proof.* (i)⇒(ii): $R$ is commutative since the generators commute. Let $G = \langle x_i + 1 \rangle$. For the generators of $G$, we have $n(x_i + 1) = nx_i + n = n$ and $(x_i + 1)(x_j + 1) = 0 + x_i + x_j + 1 = (x_i + 1) + (x_j + 1) - 1$ and we use Lemma 4.1. The products and inverses are then straightforward.

(ii)⇒(i): Let $X = \{x \in R;\ x + 1 \in G\}$. Now, $R$ is generated by $X$ and $nx = n(x + 1) - n = n - n = 0$, for each $x \in R$. Finally, for all $x, y \in R$, we have $(x + 1)(y + 1) = x + 1 + y + 1 - 1 = x + y + 1$ due to (ii). On the other hand $(x + 1)(y + 1) = xy + x + y + 1$, which yields $xy = 0$. □

The construction given in Proposition 3.4 was based on the assumption that $\varphi$ is a bilinear form. We can generalize the construction, assuming bilinear mappings and results from Lemma 4.2. Proposition 3.4 can be then obtained from Theorem 4.3 putting $K = \mathbb{Z}_{mn^2}$ and $X = \{mn\}$. In the sequel, $\mathbb{Z}_0$ means $\mathbb{Z}$ and kernel of a set of homomorphisms means the intersection of all the kernels.

**Theorem 4.3.** *Let $K$ be an abelian group and let $n \in N$. Let $X$ be a subset of* $\mathrm{End}(K)$ *satisfying $nX = X^2 = 0$. Denote $G = \langle X + \mathrm{id}_K \rangle_{\mathrm{Aut}\, K}$. Then $G$ is a $\mathbb{Z}_n$ module. Let $\varphi$ be a symmetric bilinear mapping $H^2 \mapsto G$. Then $K \rtimes_\varphi H$ is a commutative A-loop.*

*$N_\mu(K \rtimes_\varphi H) = K \times \mathrm{Rad}\, \varphi$ and $N_\lambda(K \rtimes_\varphi H) = \mathrm{Ker}(\mathrm{Im}\, \varphi - \mathrm{id}_K) \times \mathrm{Rad}\, \varphi$.*

*Proof.* $G$ is an abelian group by Lemma 4.2. $G$ is of exponent dividing $n$ because $(x + 1)^n = nx + 1 = 1$, for each $x \in X$. Property (1) comes from the symmetry. Property (3) from the commutativity of $G$. Properties (2) and (4) come from the bilinearity of $\varphi$. Property (5) is guaranteed by Lemma 4.2.

By Proposition 1.4, $(a, i) \in N_\mu(Q)$ if and only if $\varphi_{i,j} = \mathrm{id}_K$, for each $j \in H$ which is equivalent to $i \in \mathrm{Rad}\, \varphi$. And $(a, i) \in N_\lambda(Q)$ if $(a, i) \in N_\mu(Q)$ and $\varphi_{j,k}(a) = a$, for all $j, k \in H$, the latter being equivalent to $a \in \mathrm{Ker}(x - \mathrm{id}_K)$, for each $x \in \mathrm{Im}\, \varphi$. □

**Example 4.4.** Let $K$ and $H$ be vector spaces over a field $F$ of characteristic $n$. Denote by $M_{i,j}$ the matrix with 1 on position $i, j$ and 0 elsewhere. Let $X$ be a subset of $\{M_{i,j}\}$ satisfying that $M_{i,j}$ and $M_{k,l}$ lie in $X$ only if $i \neq l$ and $j \neq k$. Then $nX = X^2 = 0$. Moreover, $G = \langle X + 1 \rangle_{\mathrm{Aut}\, K}$ is an elementary abelian $n$-group and therefore $\varphi$ can be viewed as a symmetric bilinear vector space homomorphism from $H^2$ to $G$.

In the end we focus on a specific case of Example 4.4, namely $|X| = 1$. The reason is that we want to describe all commutative A-loops of order $p^3$ that can be constructed as semidirect products.

**Lemma 4.5.** *Let $K$ and $H$ be vector spaces over a field $F$,* $\dim H = 1$. *Let $x, y \in \mathrm{End}(K)$ such that $x^2 = y^2 = 0$. Let there exist $g$, an automorphism of $K$, such that $gx = yg$. Let $\varphi : H^2 \mapsto \langle x + \mathrm{id}_K \rangle$ and $\psi : H^2 \mapsto \langle y + \mathrm{id}_K \rangle$ be two nontrivial bilinear mappings. Then $K \rtimes_\varphi H \cong K \rtimes_\psi H$.*

*Proof.* We define $q, r$ as follows: $\varphi_{1,1} = qx + \mathrm{id}_K$ and $\psi_{1,1} = ry + \mathrm{id}_K$. Then clearly $\varphi_{i,j} = qijx + \mathrm{id}_K$ and $\psi_{i,j} = rijy + \mathrm{id}_K$. We define an automorphism $f$ on $K$ as

$$f = \begin{cases} r \cdot g & \text{on } \mathrm{Ker}\, x \\ q \cdot g & \text{on a complement of } \mathrm{Ker}\, x \end{cases}$$

We claim that $qfx = ryf$. Indeed, $qfx = qrgx = rqyg$ since $\operatorname{Im} x \subseteq \operatorname{Ker} x$. And $qyg = yf$ since $\operatorname{Ker} y = f(\operatorname{Ker} x)$. Now $\gamma : (a, i) \mapsto (f(a), i)$ is the searched automorphism.

$$\begin{aligned}\gamma((a,i) * (b,j)) &= \gamma((\varphi_{i,j}(a+b), i+j)) = \gamma(((qijx+1)(a+b), i+j)) \\ &= (f(qijx + \mathrm{id}_K)(a+b), i+j) \\ \gamma((a,i)) * \gamma((b,j)) &= (f(a),i) * (f(b),j) = (\psi_{i,j}(f(a+b)), i+j) \\ &= ((rijy + \mathrm{id}_K)(f(a+b)), i+j)\end{aligned}$$

□

**Example 4.6.** Let $K = \mathbb{Z}_p^2$, $H = \mathbb{Z}_p$ and $X = \{x\}$, for some $x \in \operatorname{End}(K)$ with $x^2 = 0$. The corresponding semidirect product is associative if and only if $x$ is the zero endomorphism. If $x$ is non-trivial than different choices of $x$ and $\varphi$ yield isomorphic loops—all the usable nonzero endomorphisms of $K$ are $\left(\begin{smallmatrix} 0 & a \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 \\ a & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} a & a \\ -a & -a \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} a & -a \\ a & -a \end{smallmatrix}\right)$, for some $a \in K$, and it is easy to check that all these matrices are similar and give isomorphic loops due to Lemma 4.5.

Finally comes the classification of all commutative A-loops of order $p^3$ that can be obtained as semidirect products. We summarise results of Examples 3.9 and 4.6.

**Proposition 4.7.** *For each prime $p$, there exists at least five non-isomorphic commutative A-loops of order $p^3$ that are semidirect products:*

1. *Groups $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ and $\mathbb{Z}_p^3$,*
2. *Loop constructed from Theorem 4.3 using $K = \mathbb{Z}_{p^2}$, $H = \mathbb{Z}_p$ $X = \{p\}$ and $\varphi = I$;*
3. *Loop constructed from Theorem 4.3 using $K = \mathbb{Z}_{p^2}$, $H = \mathbb{Z}_p$ $X = \{p\}$ and $\varphi$ non-equivalent to $I$, for $p$ odd;*
4. *Loop constructed from Theorem 4.3 using $K = \mathbb{Z}_p^2$, $H = \mathbb{Z}_p$, $X = \{x\}$, where $x$ is a non-zero endomorphisms with $x^2 = 0$;*
5. *Semidirect product of $K = \mathbb{Z}_2^2$, $H = \mathbb{Z}_2$ and $\varphi_{1,1} = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.*

*Proof.* It was shown earlier that all these constructions are commutative A-loops of order $p^3$. It remains to prove that they are not isomorphic. (5) has trivial left nucleus, unlike all the others. (2) and (3) have middle nuclei isomorphic to $\mathbb{Z}_{p^2}$ and (4) has middle nucleus isomorphic to $\mathbb{Z}_p^2$. (2) and (3) are not isomorphic due to Proposition 3.6. □

Actually, there are *exactly* five commutative A-loops of order $p^3$ constructable as semidirect products and therefore the list is complete. The reason is the following: it was proved in [1] that there are exactly 7 commutative A-loops of order $p^3$. One of them is the cyclic group $Z_{p^3}$ that is obviously not a semidirect product. Moreover, for each prime $p$, there exists one more loop that is not a semidirect product. However, we do not prove it here as it is out of the scope of this paper.

## References


[1] D. A. S. de Barros, A. Grishkov, P. Vojtěchovský: *Commutative automorphic loops of order $p^3$*, accepted to J. Alg. App.

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

[3] A. Drápal: *A class of commutative loops with metacyclic inner mapping groups*, Comment. Math. Univ. Carolin. **49**,3 (2008) 357–382.

[4] S. Gagola III: *Cyclic extensions of Moufang loops induced by semi-automorphisms*, submitted

[5] P. Jedlička, M. Kinyon, P. Vojtěchovský: *Structure of commutative automorphic loops*, Trans. of AMS 363 (2011), no. 1, 365–384
[6] P. Jedlička, M. Kinyon, P. Vojtěchovský: *Constructions of commutative automorphic loops*, Commun. in Alg., vol. 38 Issue 9 (2010), 3243–3267
[7] P. Jedlička, D. Simon: *On commutative A-loops of order pq*, to appear in Comm. in Alg.
[8] G. P. Nagy, P. Vojtěchovský: *LOOPS: Computing with quasigroups and loops*, version 2.0.0, package for GAP, `http://www.math.du.edu/loops`
[9] H. O. Pflugfelder: "Quasigroups and Loops: Introduction" (1990) Berlin: Heldermann

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