Odd order semidirect extensions of commutative automorphic loops

Přemysl Jedlička

Abstract. We analyze semidirect extensions of middle nuclei of commutative automorphic loops. We find a less complicated conditions for the semidirect construction when the middle nucleus is an odd order abelian group. We then use the description to study extensions of orders 3 and 5.

Keywords: automorphic loop; semidirect product; middle nucleus; cyclic group

Classification: 20N05

An automorphic loop is a loop where all inner mappings are automorphisms. Most of the basic properties of commutative automorphic loops were described in [3].

In [2], Jan Hora and the author described semidirect extensions of middle nuclei of commutative automorphic loops by abelian groups. Furthermore a few examples of specific loops were showed, mostly assuming that the middle nucleus is a small group. In this paper, on the contrary, we assume that the factor over the nucleus is a small cyclic group. The case of the middle nucleus of index 2 was already resolved in [4] and therefore we decided to focus on small odd primes.

In Section 1 we recall the notion of the semidirect product. In Section 2 we study the commutative automorphic loops with the middle nucleus of index 3 and, if the middle nucleus is not a complicated group, we count the number of such loops up to isomorphism. In order to analyze extension by larger groups, we investigate the general extensions by uniquely 2-divisible groups in Section 3, deducing shorter conditions for the semidirect product. We use this conditions in Section 4 to study extensions of order 5.

1. Preliminaries

We expect the reader to be already familiar with basic definitions in the loop theory. If not, we refer to [6]. Unlike 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 rings.

In this section, we shall recall the semidirect construction presented in [2]. 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 [2] an external point of view was given, assuming additionally that $K \leq N_\mu(Q)$ and K being an abelian group. Such loops can be constructed given a special mapping φ.

Proposition 1 ([2]). *Let H and K be abelian groups and let us have a mapping $\varphi : H^2 \to \operatorname{Aut}(K)$. 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 $N_\lambda = \{a \in K;\ \forall j,k \in H :\ \varphi_{j,k}(a) = a\} \times \{i \in H;\ \forall j \in H :\ \varphi_{i,j} = \mathrm{id}_K\}$.

The question of isomorphism classes was not tackled in [2] and hence we have to show it here.

Proposition 2. *Let $Q_1 = K \rtimes_\varphi H$ and $Q_2 = K \rtimes_\psi H$ be two semidirect products such that, for each $i \in H$, there exists $j \in H$ such that $\varphi_{ij} \neq \mathrm{id}_K$. Then $Q_1 \cong Q_2$ if and only if there exist $\alpha \in \operatorname{Aut}(K)$ and $\beta \in \operatorname{Aut}(H)$ such that $\alpha\varphi_{i,j} = \psi_{\beta(i),\beta(j)}\alpha$, for all $i, j \in H$.*

Proof: "$\Leftarrow$". An isomorphism is the mapping $f : (a,i) \mapsto (\alpha(a), \beta(i))$.

$$\begin{aligned} f((a,i)) *_2 f((b,j)) &= (\alpha(a), \beta(j)) *_2 (\alpha(b), \beta(j)) = (\psi_{\beta(i),\beta(j)}\alpha(a+b), \beta(i+j)) \\ f((a,i) *_1 (b,j)) &= f(\varphi_{i,j}(a+b), i+j) = (\alpha\varphi_{i,j}(a+b), \beta(i+j)). \end{aligned}$$

"$\Rightarrow$". Since $\varphi_{i,\_}$ is never trivial, the middle nucleus of Q_1 is $K \times 0$. Let f be an isomorphism $Q_1 \to Q_2$. Then f sends $N_\mu(Q_1)$ to $N_\mu(Q_2)$. We denote by α the restriction of f on $K \times 0$. Moreover, we define mappings $\beta : H \to H$ and $\gamma : H \to K$ to satisfy $f((0,i)) = (\gamma(i), \beta(i))$. We have

$$\begin{aligned} (\gamma(i+j), \beta(i+j)) &= f((0, i+j)) = f((0,i) *_1 (0,j)) = f((0,i)) *_2 f((0,j)) \\ &= (\gamma(i), \beta(i)) *_2 ((\gamma(j), \beta(j))) = (\psi_{\beta(i),\beta(j)}(\gamma(i) + \gamma(j)), \beta(i+j)) \end{aligned}$$

and therefore the mapping β is a homomorphism; it is a bijection too since f is a bijection on the set of cosets of $K \times 0$. Moreover, we see $\gamma(i) + \gamma(j) = \psi^{-1}_{\beta(i),\beta(j)}\gamma(i+j)$.

Now we compute

$$f((a,i)) = f((a,0) *_1 (0,i)) = (\alpha(a),0) *_2 (\gamma(i),\beta(i)) = (\alpha(a)+\gamma(i),\beta(i)).$$

We finally compute

$$\begin{aligned} f((a,i)) *_2 f((b,j)) &= (\alpha(a)+\gamma(i),\beta(i)) *_2 (\alpha(b)+\gamma(i),\beta(i)) \\ &= (\psi_{\beta(i),\beta(j)}(\alpha(a+b)+\gamma(i)+\gamma(j)),\beta(i+j)), \\ f((a,i) *_1 (b,j)) &= f(\varphi_{i,j}(a+b),i+j) = (\alpha(\varphi_{i,j}(a+b)+\gamma(i+j)),\beta(i+j)). \end{aligned}$$

If $a+b=0$ then $\alpha\gamma(i+j) = \psi_{\beta(i),\beta(j)}(\gamma(i)+\gamma(j)) = \gamma(i+j)$ and α fixes the image of γ. Now $f((a,i)) *_2 f((b,j)) = f((a,i) *_1 (b,j))$ if and only if $\psi_{\beta(i),\beta(j)}(\alpha(a+b)) = \alpha(\varphi_{i,j}(a+b))$. □

It is worth noting that the condition demanding $\varphi_{i,\_}$ to be non-trivial is sufficient but not necessary for the existence of the automorphism; it was actually not needed in the proof of the "only if" part.

A finite abelian group is a product of its prime components. Moreover, any automorphism of the group splits on the prime components. It is hence useful to know the impact of the splitting on the semidirect product.

Proposition 3. *Let $K = K_1 \times K_2$ and suppose that φ splits on K, meaning that, there exist $\bar{\varphi} : H^2 \to \mathrm{Aut}(K_1)$ and $\bar{\bar{\varphi}} : H^2 \to \mathrm{Aut}(K_2)$ such that $\varphi_{i,j}((a_1,a_2)) = (\bar{\varphi}_{i,j}(a_1), \bar{\bar{\varphi}}_{i,j}(a_2))$, for each $i,j \in H$. Then $K \rtimes_\varphi H$ is the pullback of $K_1 \rtimes_{\bar{\varphi}} H$ and $K_2 \rtimes_{\bar{\bar{\varphi}}} H$. In particular, if $\bar{\varphi}$ is trivial then $K \rtimes_\varphi H \cong K_1 \times (K_2 \rtimes_{\bar{\bar{\varphi}}} H)$.*

Proof: We recall the definition of a pullback: suppose that A, B, C are two groupoids with homomorphisms $f : A \to C$ and $g : B \to C$. The pullback is the groupoid $A \times_C B = \{(a,b);\ a \in A,\ b \in B,\ f(a) = g(b)\}$.

In our context, $A = K_1 \rtimes_{\bar{\varphi}} H$, $B = K_2 \rtimes_{\bar{\bar{\varphi}}} H$, $C = H$, and f,g are the natural projections. Denote by $Q = K \rtimes_\varphi H$. The isomorphism $A \times_C B \cong Q$ should be $h : ((a_1,i),(a_2,i)) \mapsto ((a_1,a_2),i)$. The mapping is clearly a bijection, we only prove that h is a homomorphism:

$$\begin{aligned} h(((a_1,i),(a_2,i)) * ((b_1,j),(b_2,j))) &= h((\bar{\varphi}_{i,j}(a_1+b_1),i+j),(\bar{\bar{\varphi}}_{i,j}(a_2+b_2),i+j)) \\ &= ((\bar{\varphi}_{i,j}(a_1+b_1),\bar{\bar{\varphi}}_{i,j}(a_2+b_2)),i+j) \\ &= (\varphi_{i,j}((a_1+b_1,a_2+b_2)),i+j) = ((a_1,a_2),i) * ((b_1,b_2),j) \\ &= h((a_1,i),(a_2,i)) * h((b_1,j),(b_2,j)). \end{aligned}$$

The particular case is clear. □

2. Extension of order 3

The goal of the article is to understand semidirect extensions by cyclic groups of an odd order. In this section, we start with semidirect extensions by groups of order 3. This case is rather simple and therefore it will be tackled directly, without a deeper theory. From now on, we expect K, H and φ to play the same role as in Section 1. Moreover K will be understood to wear a ring structure and we shall identify elements of K with their multiplication endomorphisms (and, in particular, 1 with the identity mapping).

Proposition 4. *Let $H = \mathbb{Z}_3$. Then ϕ satisfies conditions* (1)–(5) *if and only if there exists an automorphism α of K such that $4\alpha^2 - 5\alpha + 1 = 0$, $\phi_{1,2} = \phi_{2,1} = \alpha$ and $\varphi_{1,1} = \varphi_{2,2} = 2\alpha - 1$.*

PROOF: "$\Rightarrow$". Setting $i = j = 1$ and $k = 2$ in (5), we get $\varphi_{2,2} + 2 = 1 + 2 \cdot 1 \cdot \varphi_{1,2}$, which means $\varphi_{2,2} = 2\varphi_{1,2} - 1$. Setting $i = j = 2$ and $k = 1$, we get $\varphi_{1,1} + 2 = 1 + 2 \cdot 1 \cdot \varphi_{1,2}$, which means $\varphi_{1,1} = 2\varphi_{1,2} - 1$. Hence $\varphi_{1,1} = \varphi_{2,2}$.

Now, setting $i = j = k = 1$, we get $3\varphi_{1,2} = 1 + 2\varphi_{1,2}\varphi_{1,1}$. Substituting $\varphi_{1,1} = 2\varphi_{1,2} - 1$, we get $3\varphi_{1,2} = 1 + 2\varphi_{1,2}(2\varphi_{1,2} - 1)$ and this leads to $4\varphi_{1,2}^2 - 5\varphi_{1,2} + 1 = 0$.

"$\Leftarrow$". Properties (1)–(3) are clear. For (4) we have $\varphi_{2,2}\varphi_{1,1} = (2\alpha - 1)^2 = 4\alpha^2 - 4\alpha + 1 = \alpha = \varphi_{1,0}\varphi_{1,2}$. The other non-trivial option is similar.

Property (5) is trivially fulfilled, if one of the indices is 0. Suppose now $i = j = k$. Then $3\varphi_{i,2i} = 3\alpha$ and $1 + 2\varphi_{i,2i}\varphi_{i,i} = 1 + 2\alpha(2\alpha - 1) = 1 + 4\alpha^2 - 2\alpha$ and both sides are equal. If $i = j = 2k$ then $\varphi_{2i,2i} + 2 = 2\alpha + 1 = 1 + 2\varphi_{i,2i}$. □

Lemma 5. *Let $Q_1 = K \rtimes_\varphi \mathbb{Z}_3$ and $Q_2 = K \rtimes_\psi \mathbb{Z}_3$ be two automorphic loops. Then $Q_1 \cong Q_2$ if and only if $\varphi_{1,2}$ and $\psi_{1,2}$ are conjugate in* $\mathrm{Aut}(K)$.

PROOF: If $\varphi_{1,2} = \alpha\psi_{1,2}\alpha^{-1}$ then, according to Proposition 4, $\varphi_{i,j} = \alpha\psi_{j,i}\alpha^{-1}$, for any $i, j \in \mathbb{Z}_3$ and Q_1 and Q_2 are isomorphic due to Proposition 2.

On the other hand, if $\varphi_{1,2} = 1$ then φ is trivial, according to Proposition 4, and the resulting loop is a direct product. But this means that ψ is trivial too and $\varphi_{1,2} = \psi_{1,2}$.

Suppose hence $\varphi_{1,2} = \varphi_{2,1} \neq 1$. Proposition 4 states, that $\psi_{i,j} = \psi_{\beta(i),\beta(j)}$, for both the possible automorphisms β and any $i, j \in \mathbb{Z}_3$. Now, if $\alpha\varphi_{1,2} = \psi_{1,2}\alpha$ then $\alpha\varphi_{1,1} = \psi_{1,1}\alpha$ since $\varphi_{1,1}$ and $\psi_{1,1}$ are already determined. □

If K is a ring with a transparent structure, we can easily count the number of loops so obtained.

Proposition 6. *Let K be a vector space over a field F of dimension n. If* $\mathrm{char}(F) = 2$ *then every semidirect product $K \rtimes \mathbb{Z}_3$ yielding an automorphic loop is direct. If* $\mathrm{char}(F) = 3$ *then there exist, up to isomorphism, $\lceil \frac{n}{2} \rceil$ semidirect products $K \rtimes \mathbb{Z}_3$ that are automorphic loops. Otherwise, there are $n + 1$ such loops, up to isomorphism.*

PROOF: The case of characteristic 2 is trivial since the equation $4\alpha^2 - 5\alpha + 1 = 0$ reduces to $\alpha = 1$. We shall hence suppose different characteristic.

Let α now be a solution of the quadratic equation $4x^2 - 5x + 1 = 0$. The minimal polynomial of α divides $4x^2 - 5x + 1$ and therefore, if the characteristic differs from 3, α is similar to a diagonal matrix with entries in $\{1, \frac{1}{4}\}$. There are $n + 1$ such matrices, up to similarity, which is, according to Lemma 5, the only criterion for an isomorphism.

In characteristic 3, the roots are not distinct since $\frac{1}{4} = 1$. On the other hand, we can use the Jordan blocks $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. $\square$

It is useful to note that, in the previous case, the fundamental loop construction is the semidirect product $K \rtimes_{\varphi} \mathbb{Z}_3$ with $\dim K = 2$ and $\varphi_{1,2} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ in characteristic 3 and $\dim K = 1$ and $\varphi_{1,2} = \frac{1}{4}$ in different characteristic. The other constructions can be obtained using pullbacks and direct products as stated in Proposition 3.

Next we shall focus on rings $\mathbb{Z}_p^k$. A standard tool for computing roots of polynomials modulo p^k is Hensel's lemma:

Lemma 7 (Hensel)**.** *Let f be a polynomial in $\mathbb{Z}[x]$, let p be a prime, let $m, k \in \mathbb{N}$ and let $r \in \mathbb{Z}$ such that*

$$f(r) \equiv 0 \pmod{p^k} \qquad \text{and} \qquad f'(r) \not\equiv 0 \pmod{p^k}.$$

Then there exists $s \in \mathbb{Z}$ such that

$$f(s) \equiv 0 \pmod{p^{k+m}} \qquad \text{and} \qquad r \equiv s \pmod{p^k}.$$

Moreover, such s is unique modulo p^{k+m}.

Proposition 8. *Let $K = \mathbb{Z}_{p^k}$, for some odd prime k. Then there exist two non-isomorphic automorphic loops $\mathbb{Z}_{p^k} \rtimes_{\varphi} \mathbb{Z}_3$ for $p > 3$, one for $p^k = 3$, three for $p^k = 9$ and six such loops if $p = 3$ and $k > 2$.*

Proof: Every automorphism is equivalent to multiplication by an invertible element and all the automorphisms commute. Hence distinct automorphisms never conjugate and different constructions give rise to different loops, according to Lemma 5. If $p > 5$ then the polynomial $4x^2 - 5x + 1$ from Proposition 4 has two distinct roots, according to Hensel's lemma.

In $\mathbb{Z}_3$ there is only one root. In $\mathbb{Z}_9$ we have three roots, namely 1, 4 and 7. Suppose now $p = 3$ and $k > 2$. We compute first all the roots x of the form $x = 9y + 1$, where $y \in [0, 3^{k-2} - 1]$.

$$4 \cdot (9y+1)^2 - 5 \cdot (9y+1) + 1 = 324y^2 + 27y = 27y \cdot (12y+1).$$

This expression is congruent to 0 modulo p^k if and only if $y \cdot (12y+1) \equiv 0 \pmod{3^{k-3}}$, that means if and only if $y \equiv 0 \pmod{3^{k-3}}$ and there are exactly 3 such options, namely 0, 3^{k-3} and $2 \cdot 3^{k-3}$.

Now comes $x = 9y + 4$, where $y \in [0, 3^{k-2})$.

$$4 \cdot (9y+4)^2 - 5 \cdot (9y+4) + 1 = 324y^2 + 243y + 25 = 27 \cdot (12y^2 + 9y + 1) + 9$$

and we see that these numbers are not congruent to 0 modulo 27.

Let us take finally $x = 9y + 7$, where $y \in [0, 3^{k-2})$.

$$4 \cdot (9y+7)^2 - 5 \cdot (9y+7) + 1 = 324y^2 + 459y + 162 = 27 \cdot (12y^2 + 17y + 6).$$

This expression is congruent to 0 modulo 3^k if and only if $12y^2 + 17y + 6 \equiv 0 \pmod{3^{k-3}}$. The polynomial $12y^2 + 17y + 6$ is linear modulo 3 and its only root can be lifted using Hensel's lemma giving a unique root in $[0, 3^{k-3})$. Hence we obtain three solutions in $[0, 3^{k-2})$ again. □

It was already observed in Proposition 3 that the decomposition of K gives the decomposition of $K \rtimes_\varphi H$ as a pullback. This means that the only case left to count the number of different $K \rtimes_\varphi \mathbb{Z}_3$, for an arbitrary finite K, is the case $K \cong \prod \mathbb{Z}_{p^{e_i}}$. However this would need the description of conjugacy classes of isomorphisms in such groups and this is out of the scope of this article.

3. Extension of 2-divisible groups

It was shown in [3] that a finite commutative automorphic loop always splits as a direct product of a 2-loop and a uniquely 2-divisible loop (a loop is *uniquely 2-divisible*, if the mapping $x \mapsto x + x$ is a bijection). In this paper, we are interested in extensions of finite commutative automorphic loops by odd order abelian loops and the only way how to extend a 2-loop with an odd order group is then the trivial one. We can thus assume that every abelian group, taking place here from now on, is uniquely 2-divisible.

In this section we analyze the semidirect extensions by uniquely 2-divisible loops and we present simpler conditions to replace conditions (1)–(5).

Lemma 9. *Let φ satisfy (1)–(5). Then*

$$\varphi_{i,j} = \varphi_{-i,-j} = \frac{\varphi_{i+j,-i-j} + \varphi_{i,-i} + \varphi_{j,-j} - 1}{2\varphi_{i+j,-i-j}}, \tag{6}$$

for any $i, j \in H$.

Proof: Putting $j = i$ and $k = -i-j$ in (5) we obtain $\varphi_{i+j,-i-j} + \varphi_{i,-i} + \varphi_{j,-j} = 1 + 2\varphi_{i+j,-i-j}\varphi_{i,j}$ and hence $\varphi_{i,j} = (\varphi_{i+j,-i-j} + \varphi_{i,-i} + \varphi_{j,-j} - 1) \circ \varphi^{-1}_{i+j,-i-j}/2$. Substituting $i \to -i$ and $j \to -j$ gives the same expression due to symmetry. □

Lemma 9 states that, for a uniquely 2-divisible group K, any $\varphi_{i,j}$ can be expressed in terms of mappings $\varphi_{k,-k}$; for the sake of brevity, we shall write φ_k as an abbreviation for $\varphi_{k,-k}$. Note that $\varphi_i = \varphi_{-i}$.

It is now necessary to express conditions (1)–(5) in terms of mappings φ_k; there are much less automorphisms to check and it is possible that new induced conditions may be simpler. For this, we need to find alternative expressions for products and for $\varphi_{i,j,k}$.

Lemma 10. *Let $i, j, k \in H$ and let φ satisfy (1)–(5). Then*

$$4\varphi_i\varphi_j = 2\varphi_i + 2\varphi_j + \varphi_{i+j} + \varphi_{i-j} - 2, \tag{7}$$

$$\varphi_{i,j,k} = \frac{\varphi_i + \varphi_j + \varphi_k + \varphi_{i+j} + \varphi_{i+k} + \varphi_{j+k} + \varphi_{i+j+k} - 3}{4\varphi_{i+j+k}}. \tag{8}$$

Moreover, (1), (2), (3), (6) and (7) are only needed to prove (8).

Proof: We set $k=-j$ in (5) to obtain

$$\begin{gathered}\varphi_{i+j,-j}+\varphi_{i,0}+\varphi_{j,i-j}=1+2\varphi_{j,-j}\circ\varphi_{i,0}\\ \frac{\varphi_i+\varphi_{i+j}+\varphi_j-1}{2\varphi_i}+1+\frac{\varphi_i+\varphi_j+\varphi_{i-j}-1}{2\varphi_i}=1+2\varphi_j\\ \varphi_i+\varphi_{i+j}+\varphi_j-1+\varphi_i+\varphi_j+\varphi_{i-j}-1=4\varphi_i\varphi_j\end{gathered}$$

which is (7). For (8) we compute

$$\begin{aligned}
4\varphi_{i+j+k}\varphi_{i,j,k} &= 4\varphi_{i+j+k}\varphi_{i,j}\varphi_{i+j,k}\\
&= 4\varphi_{i+j+k}\cdot\frac{\varphi_{i+j}+\varphi_i+\varphi_j-1}{2\varphi_{i+j}}\cdot\frac{\varphi_{i+j+k}+\varphi_{i+j}+\varphi_k-1}{2\varphi_{i+j+k}}\\
&= 4(\varphi_{i+j}\varphi_{i+j+k}+\varphi_{i+j}^2+\varphi_{i+j}\varphi_k-\varphi_{i+j}+\varphi_i\varphi_{i+j+k}+\varphi_i\varphi_{i+j}\\
&\qquad+\varphi_i\varphi_k-\varphi_i+\varphi_j\varphi_{i+j+k}+\varphi_j\varphi_{i+j}\\
&\qquad+\varphi_j\varphi_k-\varphi_j-\varphi_{i+j+k}-\varphi_{i+j}-\varphi_k+1)/(4\varphi_{i+j})\\
&= \varphi_{i+j+k}+\varphi_{i+j}+\varphi_k-1+\varphi_i+\varphi_j-1+4(\varphi_i\varphi_{i+j+k}+\varphi_i\varphi_k\\
&\qquad-\varphi_i+\varphi_j\varphi_{i+j+k}+\varphi_j\varphi_k-\varphi_j-\varphi_{i+j+k}-\varphi_k+1)/(4\varphi_{i+j})\\
&= \varphi_{i+j+k}+\varphi_{i+j}+\varphi_k+\varphi_i+\varphi_j-2+(2\varphi_i+2\varphi_{i+j+k}+\varphi_{2i+j+k}\\
&\qquad+\varphi_{j+k}-2+2\varphi_i+2\varphi_k+\varphi_{i+k}+\varphi_{i-k}-2-4\varphi_i+2\varphi_j\\
&\qquad+2\varphi_{i+j+k}+\varphi_{i+2j+k}+\varphi_{i+k}-2+2\varphi_j+2\varphi_k+\varphi_{j+k}\\
&\qquad+\varphi_{j-k}-2-4\varphi_j-4\varphi_{i+j+k}-4\varphi_k+4)/(4\varphi_{i+j})\\
&= \varphi_{i+j+k}+\varphi_{i+j}+\varphi_k+\varphi_i+\varphi_j-2+(\varphi_{2i+j+k}\\
&\qquad+2\varphi_{j+k}+2\varphi_{i+k}+\varphi_{i-k}+\varphi_{i+2j+k}+\varphi_{j-k}-4)/(4\varphi_{i+j})\\
&= \varphi_{i+j+k}+\varphi_{i+j}+\varphi_k+\varphi_i+\varphi_j-3+(2\varphi_{i+j}+2\varphi_{i+k}+\varphi_{2i+j+k}\\
&\qquad+\varphi_{j-k}-2+2\varphi_{i+j}+2\varphi_{j+k}+\varphi_{i+2j+k}+\varphi_{i-k}-2)/(4\varphi_{i+j})\\
&= \varphi_{i+j+k}+\varphi_{i+j}+\varphi_k+\varphi_i+\varphi_j-3+(4\varphi_{i+j}\varphi_{i+k}+4\varphi_{i+j}\varphi_{j+k})/(4\varphi_{i+j})\\
&= \varphi_{i+j+k}+\varphi_{i+j}+\varphi_k+\varphi_i+\varphi_j-3+\varphi_{i+k}+\varphi_{j+k}
\end{aligned}$$ □

Theorem 11. *Let K and H be uniquely 2-divisible abelian groups and let $\varphi : H^2\to\mathrm{Aut}(K)$. Then φ satisfies condition (1) to (5) if and only if*

(6) $$\varphi_{i,j}=\frac{\varphi_{i+j}+\varphi_i+\varphi_j-1}{2\varphi_{i+j}},$$

(7) $$4\varphi_i\varphi_j=2\varphi_i+2\varphi_j+\varphi_{i+j}+\varphi_{i-j}-2,$$

(9) $$\varphi_0=1,$$

for each $i,j\in H$, where $\varphi_i=\varphi_{i,-i}$.

Proof: The necessity of the conditions was already proved in Lemmas 9 and 10 and hence we prove the sufficiency only. Conditions (1) and (2) follow immediately from (6) and (9). Condition (7) shows that the subring generated by all the φ_i, $i \in H$ is commutative, thus giving (3). In Lemma 10 we proved (1), (2), (3), (6), (7) $\Rightarrow$ (8) and we clearly see (8) $\Rightarrow$ (4). The only remaining condition is thus (5):

$$\begin{aligned}&\varphi_{i+j,k}+\varphi_{i+k,j}+\varphi_{j+k,i}=\\&\frac{\varphi_{i+j+k}+\varphi_{i+j}+\varphi_k-1}{2\varphi_{i+j+k}}+\frac{\varphi_{i+j+k}+\varphi_{i+k}+\varphi_j-1}{2\varphi_{i+j+k}}+\frac{\varphi_{i+j+k}+\varphi_{j+k}+\varphi_i-1}{2\varphi_{i+j+k}}\\&=1+\frac{\varphi_i+\varphi_j+\varphi_k+\varphi_{i+j}+\varphi_{i+k}+\varphi_{j+k}+\varphi_{i+j+k}-3}{2\varphi_{i+j+k}}=1+2\varphi_{i,j,k}\quad\square\end{aligned}$$

4. Extension of order 5

In this section we use the result of the previous section to study semidirect extensions by the cyclic group of order 5. We keep the notation of Section 3.

Proposition 12. *Let $Q = K \rtimes_\varphi \mathbb{Z}_5$ be a semidirect product. Then Q is automorphic if and only if there exists $\alpha \in \operatorname{Aut} K$ such that $\varphi_1 = \varphi_4 = \alpha$, $\varphi_2 = \varphi_3 = 4\alpha^2 - 4\alpha + 1$ and $16\alpha^3 - 28\alpha + 13\alpha - 1 = 0$.*

Proof: "$\Rightarrow$". Setting $i = j = 1$ in (7) we get $4\varphi_1^2 = 4\varphi_1 + \varphi_2 - 1$ and therefore $\varphi_2 = 4\varphi_1^2 - 4\varphi_1 + 1$. Setting $i = 2$ and $j = 1$ in (7) we get $4\varphi_2\varphi_1 = 2\varphi_2 + 3\varphi_1 + \varphi_3 - 2$. We know that $\varphi_3 = \varphi_2 = 4\varphi_1^2 - 4\varphi_1 + 1$ and this leads to $4(4\varphi_1^2 - 4\varphi_1 + 1)\varphi_1 = 3(4\varphi_1^2 - 4\varphi_1 + 1) + 3\varphi_1 - 2$ which is eventually simplified to $16\varphi_1^3 - 28\varphi_1^2 + 13\varphi_1 - 1 = 0$.

"$\Leftarrow$". We check (7) for all combinations of i, j. If $i = 0$ or $j = 0$ then (7) holds trivially. If $i = 1$ and $j \in \{1, 4\}$ then (7) leads to $4\alpha^2 = 4\alpha + (4\alpha^2 - 4\alpha + 1) - 1$. If $i = 1$ and $j \in \{2, 3\}$ then (7) is $4\alpha(4\alpha^2 - 4\alpha + 1) = 3\alpha + 3(3\alpha^2 - 4\alpha + 1) - 2$ and this holds. The case $i = 4$ is similar to $i = 1$.

If $i = 2$ and $j \in \{2, 3\}$ then (7) gives

$$\begin{aligned}4(4\alpha^2-4\alpha+1)^2&=4(4\alpha^2-4\alpha+1)+\alpha-1\\64\alpha^4-128\alpha^3+96\alpha^2-32\alpha+4&=16\alpha^2-15\alpha+3\\64\alpha^4-128\alpha^3+80\alpha^2-17\alpha+1&=0\\(4\alpha-1)\cdot(16\alpha^3-28\alpha+13\alpha-1)&=0\end{aligned}$$

and this holds. The remaining case $i = 3$ is similar. $\square$

In the general odd cyclic case, that means when H is a cyclic group of an odd order k, it seems that there always exists a polynomial, let us say f_k, such that φ_1 is a root of the polynomial. Moreover, further calculations suggest that $f_k \equiv (x-1)^{\frac{k+1}{2}} \pmod{k}$.

Open problem. Characterize the necessary and sufficient conditions for existence of an extension with a cyclic group.

We finish the section with enumeration of the loops of type $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_5$.

Proposition 13. *Let $K = \mathbb{Z}_p$, for some odd prime p. Then there exist two non-isomorphic automorphic loops $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_5$ if and only if 5 is a quadratic residue in $\mathbb{Z}_p$. Otherwise there exists only one.*

Proof: The polynomial $f = 16x^3 - 28x^2 + 13x - 1$ can be factored as $f = (x-1)\cdot(16x^2 - 12x + 1)$. The quadratic factor has roots $\frac{3\pm\sqrt{5}}{8}$. If $\sqrt{5}$ does not exist in $\mathbb{Z}_p$ then f has only one root. Moreover, in $\mathbb{Z}_5$ we have $f \equiv (x-1)^3 \pmod 5$ and hence there exists only one root too.

Suppose now that 5 is a quadratic residue. There are 3 possible choices of φ, according to Proposition 12, namely

- $\varphi_1 = \varphi_2 = \varphi_3 = \varphi_4 = 1$,
- $\varphi_1 = \varphi_4 = \frac{3+\sqrt{5}}{8}$, $\varphi_2 = \varphi_3 = 4 \cdot (\frac{3+\sqrt{5}}{8})^2 - 4 \cdot \frac{3+\sqrt{5}}{8} + 1 = \frac{9+6\sqrt{5}+5}{16} - \frac{12+4\sqrt{5}}{8} + \frac{8}{8} = \frac{3-\sqrt{5}}{8}$,
- $\varphi_1 = \varphi_4 = \frac{3-\sqrt{5}}{8}$, $\varphi_2 = \varphi_3 = \frac{3+\sqrt{5}}{8}$.

The latter two choices give isomorphic loops due to Proposition 2; we can set $\alpha = 1$ and $\beta = 2$. Hence we have two isomorphism classes, one associative and one non-associative. □

Remark. It was proved in [5] that a non-associative commutative automorphic loop of order $5p$ with a p-element middle nucleus, for an odd prime p, exists if and only if there exists a non-trivial solution of $x^5 = 1$ in $\mathrm{GF}(p^2)$. This condition is equivalent to the condition presented here: it is well known that $x^5 - 1$ can be factored using the golden ratio $\phi = \frac{1+\sqrt{5}}{2}$ as $x^5 - 1 = (x-1)\cdot(x^2 + \phi x + 1)\cdot(x^2 - \phi^{-1}x + 1)$. A non-trivial solution of $x^5 = 1$ in $\mathrm{GF}(p^2)$ thus exists if and only if 5 is a quadratic residue in $\mathbb{Z}_5$. It is also worth mentioning that the roots of $16x^3 - 28x^2 + 13x - 1$ can be nicely expressed using the golden ratio: $\frac{3+\sqrt{5}}{8} = \frac{\phi^2}{4}$ and $\frac{3-\sqrt{5}}{8} = \frac{\phi^{-2}}{4}$.

Open problem. Find the connection between the existence of an extension by $\mathbb{Z}_p$ and the roots of $x^p - 1$.

References

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

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

[3] Jedlička P., Kinyon M., Vojtěchovský P., *Structure of commutative automorphic loops*, Trans. Amer. Math. Soc. **363** (2011), no. 1, 365–384.

[4] Jedlička P., Kinyon M., Vojtěchovský P., *Constructions of commutative automorphic loops*, Comm. Algebra **38** (2010), no. 9, 3243–3267.

[5] Jedlička P., Simon D., *On commutative A-loops of order pq*, to appear.
[6] Pflugfelder H.O., *Quasigroups and Loops: Introduction*, Heldermann, Berlin, 1990.

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

(*Received* October 24, 2013)