A NUCLEAR CONSTRUCTION OF LOOPS WITH SMALL INNER MAPPING GROUPS

ALEŠ DRÁPAL

ABSTRACT. We construct an infinite class of left conjugacy closed loops Q such that the inner mapping group $\operatorname{Inn} Q$ is a nonabelian group of order pq. The constructions are done in a broader context of loops $Q = N_\lambda N_\rho$ such that $N_\lambda = N_\mu \trianglelefteq Q$ and $\operatorname{Inn} Q$ can be embedded into the holomorph of a cyclic group.

Suppose that H and K are groups and that $\gamma_x = \gamma(x) \in \operatorname{Aut} H$ for each $x \in K$. The binary operation

$$(a, x) \cdot (b, y) = (a\gamma_x(b), xy) \text{ for all } a, b \in H \text{ and } x, y \in K$$

is a group if $\gamma : K \to \operatorname{Aut} H$ is a group homomorphism. If it is not, we get a quasigroup on $H \times K$. Throughout this paper we shall assume that $\gamma(1) = \mathrm{id}_K$, which makes $(1, 1)$ the neutral element. We hence have a loop, and this loop will be denoted by $S(H, K, \gamma)$.

We shall be looking for such γ that the inner mapping group of $S(H, K, \gamma)$ is a noncommutative group of order pq, where $p > q$ are primes.

The *multiplication group* of a loop Q is the permutation group on Q generated by all left translations $L_x : y \mapsto xy$ and right translations $R_x : y \mapsto yx$, where $x, y \in Q$. By the *inner mapping group* $\operatorname{Inn} Q$ of Q we understand the stabilizer subgroup $\{\varphi \in \operatorname{Mlt} Q;\ \varphi(1) = 1\}$.

$\operatorname{Inn} Q$ is never a nontrivial cyclic group [6]. Thus q divides $p-1$ and $\operatorname{Inn} Q$ is not commutative if it is of order pq. The solvability of $\operatorname{Mlt} Q$ for such loops was studied extensively by Niemenmaa et al. in a series of papers [8, 9, 1, 7]. It was proved in [2] that $\operatorname{Mlt} Q$ has to be always solvable, and that the structure of Q has to fulfil a number of constraints. In particular, if $|\operatorname{Inn} Q| = pq$, then $Z(Q/Z(Q)) = 1$ and $|\operatorname{Inn}(Q/Z(Q))| = pq$ as well. Assume $Z(Q) = 1$. Then Q possesses a p-element normal subgroup S such that Q/S is an abelian group of order $\leq q$.

It seems to be possible to characterize all such loops. This paper contributes to the constructive aspect of this goal by stating the conditions under which we can get such loops in the form of $S(H, K, \gamma)$. Our main interest rests in the situation when H and K are cyclic, and we shall show in Section 7 that such a situation always arises when $|\operatorname{Inn} Q| = pq$ and $Z(Q) = 1$.

Sections 1-6 are self contained, with exception of some easily verifiable material from [3] that is reproduced in Section 2 and used in Section 4. Section 7 is dependent upon Proposition 7.1, which is taken from [2].

2000 *Mathematics Subject Classification.* Primary 20N05; Secondary 08A05.

Key words and phrases. inner mapping group, loop, nucleus, left cojugacy closed.

This paper was written while the author was visiting University of Wisconsin-Madison as a Fulbright research scholar. He was also supported by institutional grant MSM 0021620839.

There exist further classes of nonassociative loops Q such that $Z(Q) = 1$ and $|\operatorname{Inn} Q| = pq$. All cases when Q is conjugacy closed are described in [4], and in [5] one can find a construction in which Q is of order $2p$. The loops constructed here are left conjugacy closed but not right conjugacy closed.

Sections 1 and 2 are concerned with general facts. In Section 1 we develop formulas for the generators of $\operatorname{Inn} Q$ if $Q = S(H, K, \gamma)$, while Section 2 starts with formulas for nuclei and the center of such loops. In this section we also state several easy facts that involve cyclic groups.

In Section 2 we shall see that if $Q = S(H, K, \gamma)$ is to fulfil our goals, then a certain subgroup of H^K has to be cyclic. Section 3 is devoted to study of such a situation. In Section 4 we shall use results of Section 3 to prove that in many cases the investigated loop has to be isomorphic to a loop on $\mathbb{Z}_m \times \mathbb{Z}_k$ with operation

$$(a, x)(b, y) = (a + (1 - s + st^x)b,\ x + y).$$

Elements $s, t \in \mathbb{Z}_m^*$ are parameters of the construction, and the rest of Section 4 and all of Sections 5 and 6 are concerned with the existence of such loops, and with questions of isotopy and isomorphism.

In Section 7 we show that these loops occur whenever Q is a loop with $|\operatorname{Inn} Q| = pq$, $Z(Q) = 1$, $N_\mu = N_\lambda \trianglelefteq Q$ and $Q = N_\lambda N_\rho$.

Let Q be a loop. We write $L(x, y)$ for $L_{xy}^{-1} L_x L_y$, $R(x, y)$ for $R_{yx}^{-1} R_x R_y$ and $T(x)$ for $R_x^{-1} L_x$. It is well known that $\operatorname{Inn} Q$ is generated by all mappings $L(x, y)$, $R(x, y)$ and $T(x)$, where $x, y \in Q$.

1. Generators

Throughout this section H and K are groups, and $\gamma_x = \gamma(x) \in \operatorname{Aut} H$ for all $x \in K$. We set $Q = S(H, K, \gamma)$, and assume $\gamma(1) = \mathrm{id}_H$.

Lemma 1.1. *If $a, b, c \in H$ and $x, y, z \in K$, then*

$$L((a, x), (b, y))(c, z) = (\gamma_{xy}^{-1} \gamma_x \gamma_y(c),\ z),$$

$$R((a, x), (b, y))(c, z) = (c\,(\gamma_{zy}(a)\gamma_z\gamma_y(a^{-1}))^{\gamma_z(b^{-1})},\ z),\ \text{ and}$$

$$T((a, x))(c, z) = (a\gamma_x(c)\gamma_{xzx^{-1}}(a^{-1}),\ xzx^{-1}).$$

Proof. For example, $R_{(a,x)} R_{(b,y)}(c, z) = R_{(a,x)}(c\gamma_z(b), zy) = (c\gamma_z(b)\gamma_{zy}(a), zyx)$, and we get the same value when $(c\gamma_z(b)\gamma_{zy}(a)\gamma_z\gamma_y(a^{-1}))\gamma_z(b^{-1}), z)$ is multiplied on the right by $(b\gamma_y(a), yx) = (b, y)(a, x)$. The other two cases can be verified in a straightforward manner as well. □

Lemma 1.2. *Assume $a, b \in H$ and $x, y \in K$. Then $T((1, x))(c, z) = (\gamma_x(c), xzx^{-1})$ for all $(c, z) \in H \times K$, and*

$$L((a, x), (b, y)) = T((1, xy))^{-1} T((1, x)) T((1, y)).$$

Proof. The first equality follows from Lemma 1.1 immediately. The lemma also implies $T((1, x))T((1, y))(c, z) = (\gamma_x\gamma_y(c), xyzy^{-1}x^{-1}) = T_{(1,xy)}(\gamma_{xy}^{-1}\gamma_x\gamma_y(c), z) = T_{(1,xy)} L((a, x), (b, y))(c, z)$. □

Corollary 1.3. *Let H and K be groups, and let γ_x be an automorphism of H for each $x \in K$, $\gamma_1 = \mathrm{id}_H$. The inner mapping group of the loop $S(H, K, \gamma)$ is generated by mappings $R((a, x), (b, y))$ and $T((a, x))$, where $a, b \in H$ and $x, y \in K$.*

We shall now narrow our interest to the case when both H and K are commutative groups. We shall use additive notation for both H and K.

Lemma 1.4. *Let H and K be abelian groups. If $a, b, c \in H$ and $x, y, z \in K$, then*

$$R((a,x),(b,y))(c,z) = (c + \gamma_{z+y}(a) - \gamma_z\gamma_y(a), z), \text{ and}$$
$$T((a,x))(c,z) = (a + \gamma_x(c) - \gamma_z(a), z).$$

Proof. This an immediate consequence of Lemma 1.1. □

For an automorphism α of H denote by $\bar{\alpha}$ the automorphism of $H \times K$, $(a,x) \mapsto (\alpha(a), x)$. If $S \subseteq \operatorname{Aut} H$, then $\bar{S} = \{\bar{\alpha};\ \alpha \in S\}$.

For a mapping $d : K \to H$ denote by $\tau(d)$ the permutation $(a,x) \mapsto (a + d(x), x)$, where $(a,x) \in H \times K$. The mappings $d : K \to H$ form an abelian group H^K.

Lemma 1.5. *Let H and K be abelian groups. Then $\bar{\alpha}\tau(d)\bar{\alpha}^{-1} = \tau(\alpha d)$, for every $d \in H^K$ and $\alpha \in \operatorname{Aut} H$.*

Proof. Indeed, $\bar{\alpha}\tau(d)\bar{\alpha}^{-1}(a,x) = \bar{\alpha}(\alpha^{-1}(a) + d(x), x) = (a + \alpha d(x), x)$, for all $(a,x) \in H \times K$. □

Proposition 1.6. *Let $H = H(+)$ and $K = K(+)$ be abelian groups, and let $\gamma : K \to \operatorname{Aut} H$ be a mapping, $\gamma(0) = \mathrm{id}_H$ and $\gamma(x) = \gamma_x \in \operatorname{Aut} H$ for each $x \in K$. Put $\Gamma = \langle \gamma(x);\ x \in K \rangle$, and denote by D the subgroup of H^K generated by all mappings $d(y,a) : x \mapsto \gamma_{x+y}(a) - \gamma_y(a)$, where $(a,y) \in H \times K$. Furthermore, let $E \le H^K$ be generated by all αd, where $\alpha \in \Gamma$ and $d \in D$. Set $Q = S(H,K,\gamma)$. Then $\operatorname{Inn} Q = \bar{\Gamma}\tau(E)$ and $\tau(E) \trianglelefteq \operatorname{Inn} Q$.*

Proof. We have $\bar{\gamma}_x \in \operatorname{Inn} Q$ for all $x \in Q$ since $T(0,x)(c,z) = (\gamma_x(c), z)$ for all $(c,z) \in H \times K$. The mapping $\alpha \to \bar{\alpha}$ yields an embedding $\operatorname{Aut} H \to \operatorname{Aut}(H \times K)$, and hence $\bar{\Gamma} \le \operatorname{Inn} Q$.

Note that $\tau(u_1 + u_2) = \tau(u_1)\tau(u_2)$ for all $u_1, u_2 \in H^K$. Choose $a, b \in H$ and $x, y \in K$. The mapping $R((a,x),(b,y))$ is equal to $\tau(u)$, where $u(z) = \gamma_{z+y}(a) - \gamma_z\gamma_y(a)$, for all $z \in Q$, by Lemma 1.4. We can express $u(z)$ as $(\gamma_{z+y}(a) - \gamma_y(a)) - (\gamma_z\gamma_y(a) - \gamma_y(a))$, which means $u = d(y,a) - d(0, \gamma_y(a))$. Hence $\tau(d(y,a)) \in \operatorname{Inn} Q$ if and only if $\tau(d(0, \gamma_y(a))) \in \operatorname{Inn} Q$.

Now, $\tau(d(0,b)) \in \operatorname{Inn} Q$ for all $b \in K$ since $T((b,0))^{-1}(c,z) = (c + \gamma_z(b) - b, z) = \tau(d(0,b))(c,z)$, for all $(c,z) \in H \times K$. Thus $\tau(D) \le \operatorname{Inn} Q$, and $\tau(E) \le \operatorname{Inn} Q$ follows from Lemma 1.5. We have proved $\bar{\Gamma}\tau(E) \le \operatorname{Inn} Q$.

To get the converse inclusion first note that we already know that $R((a,x),(b,y))$ always belongs to $\tau(D)$. The rest follows from $T((a,x)) = T((a,0))T((0,x)) = \tau d(0,-a)\bar{\gamma}_x$, by Corollary 1.3. □

Corollary 1.7. *Assume, in addition, that Γ is commutative. Then $\operatorname{Inn} Q = \bar{\Gamma}\tau(D)$, $\tau(D) \trianglelefteq \operatorname{Inn} Q$ and $\tau(D) \cap \bar{\Gamma} = 1$.*

Proof. By Lemma 1.5 it suffices to observe that $\tau(\alpha d(x,a))(c,z) = (c + \alpha(\gamma_{z+x}(a) - \gamma_x(a)), z) = (c + \gamma_{z+x}\alpha(a) - \gamma_x\alpha(a), z) = \tau(d(x, \alpha(a)))(c,z)$, for all $\alpha \in \Gamma$. □

2. Structural aspects

In every loop Q one defines the *left nucleus* N_λ as the set of those $a \in Q$ that fulfil $a(xy) = (ax)y$ for all $x, y \in Q$. By shifting a to the right we get the *middle nucleus* N_μ and the *right nucleus* N_ρ.

By Lemma 3.5 of [3] a loop Q can be obtained as a factor of some $S(H, K, \gamma)$ if $Q = (N_\lambda \cap N_\mu)N_\rho$ and $N_\lambda \cap N_\mu \trianglelefteq Q$. Here we are interested only in the structure of $S(H, K, \gamma)$, and not of its factors. To this effect [3] has something to say as well. On the basis of its Lemmas 3.1 and 3.2 we can state:

Lemma 2.1. *Assume $Q = S(H, K, \gamma)$, where H and K are groups, $\gamma(x) = \gamma_x \in \operatorname{Aut} H$ for each $x \in K$, and $\gamma(1) = \mathrm{id}_H$. Then $N_\lambda = H \times K_\lambda$, $N_\mu = H \times K_\mu$ and $N_\rho = H_\rho \times K$, where $K_\lambda = \{x \in K;\, \gamma(x)\gamma(y) = \gamma(xy)$ for all $y \in K\}$, $K_\mu = \{x \in K;\, \gamma(y)\gamma(x) = \gamma(yx)$ for all $y \in K\}$ and $H_\rho = \{a \in H;\, \gamma(x)\gamma(y)(a) = \gamma(xy)(a)$ for all $x, y \in K\}$. Furthermore, the loop Q is left conjugacy closed if and only if $\gamma(x^y) = \gamma(x)^{\gamma(y)}$ for all $x, y \in Q$.*

The lemma can be verified in a straightforward way, and so the knowledge of [3] is dispensible, in fact. While the notion of left conjugacy closedness (LCC) is not essential for this paper, it is worth noting that we often obtain loops from this well established class. Recall that Q is LCC if and only if for all $u, v \in Q$ there exists $w \in Q$ such that $L_u L_v L_u^{-1} = L_w$. LCC loops can be also described equationally, e. g. by identity $((xy)/x)z = x(y(x\backslash z))$.

Let us record an immediate consequence of Lemma 2.1.

Corollary 2.2. *Suppose that H and K are abelian groups. Then $Q = S(H, K, \gamma)$ is LCC if and only if $\Gamma = \langle \operatorname{Im} \gamma \rangle$ is an abelian group as well.*

If Q is a loop, then $u \in Q$ belongs, by definition, to the *center* $Z(Q)$ if and only if it associates and commutes with all other elements. It is well known (and easy to prove) that the presence of a commuting element in two of the nuclei forces out the presence in the third one.

Suppose that $Q = S(H, K, \gamma)$, where H and K are abelian. Then $(a, x)(b, y) = (b, y)(a, x)$ is equivalent to $a + \gamma_x(b) = \gamma_y(a) + b$. We see that (a, x) commutes with all $(b, y) = (b, 0)(0, y)$ if and only if $\gamma_y(a) = a$ for all $y \in K$ and $\gamma_x(b) = b$ for all $b \in H$.

In view of Lemma 2.1 we can thus make the following claim:

Lemma 2.3. *Let $Q = S(H, K, \gamma)$, where $H = H(+)$ and $K = K(+)$ are abelian groups, $\gamma_x = \gamma(x) \in \operatorname{Aut} H$ for each $x \in K$, and $\gamma_0 = \mathrm{id}_H$. Then $Z(Q) = H_\zeta \times K_\zeta$, where $H_\zeta = \{a \in H;\, \gamma_x(a) = a$ for all $x \in K\}$ and $K_\zeta = \{x \in K;\, \gamma(x + y) = \gamma(y)\}$ for all $y \in K\}$.*

For loops Q_i, $i \in I$, define a loop $Q = \coprod Q_i$ like in groups, i. e. as a binary operation on all (a_i) with $a_i \neq 1$ only for finitely many $i \in I$, in which $(a_i)(b_i) = (a_i b_i)$. Let us make an observation:

Lemma 2.4. *Let $Q_i = S(H_i, K, \gamma_i)$, where $\gamma_i(x) \in \operatorname{Aut}(H_i)$ and $\gamma_i(x)(1) = \mathrm{id}_{H_i}$ for all $i \in I$, $I \neq \emptyset$. Put $H = \coprod H_i$ and define $\gamma = \coprod \gamma_i : K \to \operatorname{Aut} H$ by $\gamma(x)((a_i)) = (\gamma_i(x)(a_i))$. Then $((h_i), x) \mapsto ((h_i, x))$ yields an embedding of $Q = S(H, K, \gamma)$ into $\coprod Q_i$.*

Proof. This is clear since $((h_i, x)) \cdot ((h'_i, x'))$ is equal, as a product in $\coprod Q_i$, to $((h_i\gamma_i(x)(h'_i), xx'))$, the image of $((h_i\gamma_i(x)(h'_i)), xx') = ((h_i)\gamma(x)((h'_i)), xx') \in Q$, and that is equal in Q to the product $((h_i), x) \cdot ((h'_i), x')$. □

Every automorphism acts upon each characteristic subgroup. If H is a direct sum of characteristic subgroups H_i, then each $\gamma : K \to \operatorname{Aut} H$ can be expressed as $\coprod \gamma_i$, and the above lemma can be used to illuminate the structure of $S(H, K, \gamma)$. In particular this is true when $H = H(+)$ is a torsion abelian group (which is equal to $\bigoplus H_p$, where H_p is the p-primary component, for each prime p).

Suppose that a group B acts upon a group A. Then $C_A(B) = \{a \in A;\ a^b = a$ for all $b \in B\}$ is the sugroup of A upon which B acts trivially, while $C_B(A) = \{b \in B;$ $a^b = a$ for all $a \in A\}$ describes the kernel of the action. This notation refers to centralizers within the semidirect product $A \ltimes B$, $(a', b')(a, b) = (a'a^{b'}, b'b)$. Note that $A \ltimes B$ naturally embeds into the holomorph of A if and only if $C_B(A)$ is trivial.

Lemma 2.5. *Let $G = A \ltimes B$ be a group such that A is cyclic of order m, B is abelian, and $C_A(B) = 1$. Then $A = G'$.*

Proof. Clearly $A \geq G'$. It suffices to prove the converse inclusion only for each p-primary component of A. We can thus assume that A is a nontrivial p-group, with a generator a. The order of an automorphism $a^i \mapsto a^{ij}$ is equal to a power of p if and only if $j \equiv 1 \bmod p$. Every such automorphism fixes the element $a^{m/p}$, and so our assumptions imply the existence of $b \in B$ with $a^b = a^j$ and $(j-1, p) = 1$. Now, $[a^i, b] = a^{i(j-1)}$, for each integer i, and hence every power of a is in G'. □

Lemma 2.6. *Let G be such a group that G' is abelian and equal to the kernel of the action of G upon G'. Then G' is the only abelian subgroup $A \trianglelefteq G$ such that G/A is abelian.*

Proof. Let $A \trianglelefteq G$ fulfil the asssumptions of the lemma. Clearly $A \geq G'$. Each element $a \in A \setminus G'$ is assumed to act nontrivially upon G'. Hence for every such element there exists $x \in G' \leq A$ with $[x, a] \neq 1$. However, no such element can exist if A is abelian. □

Corollary 2.7. *Let B be a group that acts faithfully upon a cyclic group A of order m. If $C_A(B) = 1$, then $A = G'$ is the only abelian subgroup of $G = A \ltimes B$ the factor over which is abelian as well.*

Proof. To apply Lemma 2.6 we need to establish $A = G'$. By Lemma 2.5 this follows from $C_A(B) = 1$. □

Lemma 2.8. *Let B be a group of order n that acts faithfully upon a cyclic group A of order m. If $(n, m) = 1$, then $C_A(B) = 1$.*

Proof. It suffices to show that B fixes pointwise only the trivial subgroup of every p-primary component of A, for every prime p. Let $a \in A$ generate the component, $|a| = p^k$. It will be enough to find $b \in B$ such that $(a^{p^h})^b \neq a^{p^h}$ for every h, $1 \leq h < k$. Choose any b with $a^b \neq a$. Then $a^b = a^j$ for some integer j such that $j \equiv j' \bmod p$, where $2 \leq j' < p$. This follows from the fact that the order of b is not divisible by p. We have $jp^h \not\equiv p^h \bmod p^k$, and hence b does not fix a^{p^h}. □

Suppose that a group B acts upon A. Call the action *fixed point free* if $C_A(B) = 1$. The following statement uses the notation and assumptions of Proposition 1.6.

Corollary 2.9. *Suppose that both H and K are cyclic, and that $\operatorname{Inn} Q$ is a group of order nm that contains a normal cyclic m-element subgroup upon which there acts faithfully an n-element subgroup. If the action is fixed point free, then D has to be a cyclic subgroup of H^K, $|D| = m$.*

Proof. Use Corollaries 1.7 and 2.7. □

3. An abstract background for the cyclicity condition

We start by assuming that both $H = H(+)$ and $K = K(+)$ are abelian groups. This will be later narrowed to the case when both are cyclic, and when the group $D = \langle d(x, a);\, (a, x) \in H \times K\rangle \le H^K$ is cyclic as well.

By definition, $d(x, a)(z) = \gamma_{z+x}(a) - \gamma_x(a)$ for all $x, z \in K$ and $a \in H$. This gives $d(x, a+b) = d(x, a)+d(x, b)$, for all $x \in K$ and $a, b \in H$. The behaviour in the second argument being transparent, we turn our attention to the first argument.

Lemma 3.1. *Fix $a \in H$ and set $\delta(x, y) = d(x, a)(y)$, for all $x, y \in K$. Then $\delta(x, y + z) = \delta(x + y, z) + \delta(x, y)$, for all $x, y, z \in H$.*

Proof. We have $\delta(x, y + z) = d(x, a)(y + z) = \gamma_{x+y+z}(a) - \gamma_x(a) = (\gamma_{x+y+z}(a) - \gamma_{x+y}(a)) + (\gamma_{x+y}(a) - \gamma_x(a)) = d(x + y, a)(z) + d(x, a)(y)$. □

We shall be now investigating mappings $\eta : K \times K \to H$ that satisfy

$$\eta(x, y + z) = \eta(x + y, z) + \eta(x, y) \text{ for all } x, y, z \in K.$$

Lemma 3.2. *Assume $x, y \in K$ and $n, m \in \mathbb{Z}$, with $m \ge 1$. Then:*

(i) $\eta(x, 0) = 0$ *and* $\eta(x, -y) = -\eta(x - y, y)$;
(ii) $\eta(nx, mx) = \sum_{0\le i<m} \eta((n + i)x, x)$; *and*
(iii) $\eta(nx, -mx) = -\sum_{0<i\le m} \eta((n - i)x, x)$.

Proof. We have $\eta(x, 0) = \eta(x, 0 + 0) = 2\eta(x, 0) = 0 = \eta(x, -y + y) = \eta(x - y, y) + \eta(x, -y)$. To get (ii) proceed by induction, starting from $m = 1$. The induction step follows from $\eta(nx,(m + 1)x) = \eta((n + m)x, x) + \eta(nx, mx)$. For (iii) use $\eta(nx, -mx) = -\eta((n - m)x, mx)$ and apply (ii). □

Lemma 3.3. *If $x \in K$ and $n, m \in \mathbb{Z}$, then*

$$\eta(nx, mx) = \eta(0,(n + m)x) - \eta(0, nx).$$

Proof. Cases $m = 0$ and $n = 0$ are clear. Assume $m = 1$. If $n \ge 1$, then $\eta(0,(n + 1)x) - \eta(0, nx) = \sum_{0\le i\le n} \eta(ix, x) - \sum_{0\le i<n} \eta(ix, x) = \eta(nx, x)$, by point (ii) of Lemma 3.2. By point (i), $\eta(x, -x) = -\eta(0, x) = \eta(0, 0) - \eta(0, x)$. If $n \le -2$, then $\eta(0,(n + 1)x) - \eta(0, nx) = -\sum_{0<i<-n} \eta(-ix, x) + \sum_{0<i\le -n} \eta(-ix, x) = \eta(nx, x)$, by point (iii).

For $m > 1$ we can proceed by induction, using $\eta(nx,(m + 1)x) = \eta(nx, mx) + \eta((n + m)x, x) = \eta(0,(n + m)x) - \eta(0, nx) + \eta(0,(n + m + 1)x) - \eta(0,(n + m)x)$.

It remains to prove $\eta(nx, -mx) = \eta(0,(n - m)x) - \eta(0, nx)$, where $m \ge 1$. This follows from the preceding part of the proof since $\eta(nx, -mx) = -\eta((n-m)x, mx)$, by point (i) of Lemma 3.2. □

Corollary 3.4. *If $x \in K$ and $i, n, m \in \mathbb{Z}$, then*

$$\eta(nx, ix) = \eta(mx, (i+n-m)x) - \eta(mx, (n-m)x).$$

Proof. From Lemma 3.3 we get that $\eta(nx, ix)$ is equal to $\eta(0, (n+i)x) - \eta(0, nx)$, which is the same as

$$\eta(0,(i+n)x)-\eta(0,mx)-\eta(0,nx)+\eta(0,mx) = \eta(mx,(i+n-m)x)-\eta(mx,(n-m)x).$$

□

It will be convenient to write $\eta(x, y)$ also as $\eta_x(y)$, for all $x, y \in K$.

Lemma 3.5. *Suppose that K is generated by an element x, that H is a cyclic group as well, and that also all mappings η_{ix}, $i \in \mathbb{Z}$, generate a cyclic subgroup of H^K. Then each η_{mx}, $m \in \mathbb{Z}$, can serve as a generator of this subgroup.*

Proof. Let the subgroup be generated by an element $\rho \in H^K$. Denote by H_0 the subgroup of H generated by all $\rho(y)$, $y \in K$, and by H_1 the subgroup generated by all $\eta_{mx}(y) = \eta(mx, y)$, $y \in K$. We have $\eta_{mx} = c\rho$ for some $c \in \mathbb{Z}$, and hence $H_1 = cH_0$. From Corollary 3.4 we see that $\eta(ix, y) \in H_1$ for all $i \in \mathbb{Z}$ and $y \in K$. That implies $H_0 = H_1$ since ρ can be expressed as a finite linear combination of some η_{ix}. If g generates H_0, then cg generates H_0 as well, and therefore there exists $c' \in \mathbb{Z}$ such that $cc'g = g$. Hence $c'\eta_{mx}(y) = c'c\rho(y) = \rho(y)$ for all $y \in K$. □

If $t \neq 1$ is an integer, then $(t^n - t^m)/(t-1)$ is equal to a sum of t^i, $i \in \mathbb{Z}$, for all $n, m \in \mathbb{Z}$. Indeed, $(t^n - t^m)/(t-1) = t^m((t^n - 1)/(t-1))$, and for $n \geq 1$ we have $(t^n - 1)/(t-1) = 1 + t + \cdots + t^{n-1}$ and

$$\frac{t^{-n}-1}{t-1} = -t^{-1}\frac{t^{-n}-1}{t^{-1}-1} = -t^{-1} - t^{-2} - \cdots - t^{-n}.$$

Hence $((t^n - t^m)/(t-1))g$ is always a well defined multiple of g when g is a torsion element of an additive abelian group such that t is coprime to $|g|$, the order of g.

Proposition 3.6. *Let H and K be cyclic groups and let $\eta : K \times K \to H$ be a mapping such that*

(1) *the set of all $\eta_u : K \to H$ generates a cyclic subgroup of H^K, and*
(2) *$\eta(u, v + w) = \eta(u + v, w) + \eta(u, v)$ for all $u, v, w \in K$.*

Furthermore, let x be a generator of K and let $g = \eta(0, x) \in H$. Then either

(A) *$\eta(u, v) = \theta(v)$ for a homorphism $\theta : K \to H$, for all $u, v \in K$, or*
(B) *$g \neq 0$, K is not of an odd order, and for all $i, j \in \mathbb{Z}$ there exists $\varepsilon(i, j) \in \{0, 1\}$ such that $\varepsilon(i, j) \equiv j(-1)^i \bmod 2$ and $\eta(ix, jx) = \varepsilon(i, j)g$, or*
(C) *The group H is finite, and there exists a (unique) integer t, $1 < t < |g|-1$, that is coprime to $|g|$, satisfies $(t^{|x|} - 1)g = g$ if K is finite, and fulfils*

$$\eta(ix, jx) = \frac{t^{i+j} - t^i}{t-1} g \text{ for all } i, j \in \mathbb{Z}.$$

On the other hand any mapping η that satisfies (A) *or* (B) *or* (C) *fulfils conditions* (1) *and* (2). *The order of g is always the same as the order of each η_{ix}, $i \in \mathbb{Z}$.*

Proof. By Lemma 3.5 there exist $t, t' \in \mathbb{Z}$ such that $\eta_x = t\eta_0$ and $\eta_0 = t'\eta_x$. By Lemma 3.3, $\eta(x, jx) = \eta_0((j+1)x) - \eta_0(x) = t\eta_0(jx)$, for all $j \in \mathbb{Z}$. Assume $j \geq 1$ and recall that g has been defined as $\eta_0(x)$. We obtain $\eta_0(jx) = \eta_0(x) + t\eta_0((j-1)x) = \sum_{0\leq i<j} t^i g$, and $\eta_0(-jx) = -t'\eta_0(x) - t'\eta_0(-(j-1)x) = -\sum_{1\leq i\leq j} t^{-1} g$.

Note that $\eta(ix, jx)$ is a multiple of g for all $i, j \in \mathbb{Z}$, by Lemma 3.3. Hence η_0 and g are of the same order, and that coincides with the order of each η_{ix}, by Lemma 3.5. Since η_x is a generator, tg must also be a generator. Hence $t \in \{-1, 1\}$ if g is of infinite order, and t is coprime to $|g|$ if g is of finite order.

If $t = 1$, then $\eta_0(jx) = jg = \eta_{ix}(jx)$ for all $i, j \in \mathbb{Z}$, by Lemma 3.3, and $\eta_0 = \eta_{ix}$ is a homomorphism $K \to H$. On the other hand, if we set $\eta(ix, y) = \theta(y)$, for all $i \in \mathbb{Z}$ and all $y \in K$, where $\theta : K \to H$ is a homomorphism of groups, then conditions (1) and (2) clearly hold.

If $g = 0$, then all η_{ix} equal the zero homomorphism. Thus we can assume $g \neq 0$. Suppose that $t = -1$. Then $\eta_0(jx)$ alternates between 0 and g, and the formula of case (B) follows from the equality of Lemma 3.3 in an immediate way. If $|x|$ is odd, then $0 = \eta_0(0) = \eta_0(|x|x) = g$. Hence x cannot be of an odd order. If it is not, then the formula of case (B) yields a well-defined mapping η, with $\eta_{ix} = (-1)^{j-i}\eta_{jx}$ for all $i, j \in \mathbb{Z}$. Observe that also $\varepsilon(i, j) = ((-1)^{i+j} - (-1)^i)/(-2)$. Thus (B) is in fact a special case of (C), and that allows us to defer the verification of condition (2). (The case (B) is stated separately since it admits the infinity of H.)

Assume now $t \notin \{-1, 1\}$. Then g (and hence also a) has to be of a finite order. This order is the same as the order of η_0, and hence $1 < t < |g| - 1$ can be assumed. From the above expressions of $\eta_0(jx)$ we see that the formula $\eta(ix, jx) = ((t^{i+j} - t^i)/(t-1))g$ holds if $i = 0$ (the text immediately preceding the proposition can be of help here). The other cases follow from Lemma 3.3 by

$$\eta(ix, jx) = \frac{1}{t-1}(t^{i+j} - 1 - t^i + 1)g = \frac{t^{i+j} - t^i}{t-1}g.$$

Therefore $\eta_{ix} = t^i\eta_0$, and that is why $t^{|x|}g$ has to equal g when K is finite. If that holds, then the definition of $\eta(ix, jx)$ by the above formula is sound. It remains to verify condition (2). Let us have $u = ix$, $v = jx$ and $w = kx$. Then $\eta(u, v+w) = ((t^{i+j+k} - t^i)/(t-1))g = ((t^{i+j+k} - t^{i+j})/(t-1))g + ((t^{i+j} - t^i)/(t-1))g = \eta(u+v, w) + \eta(u, v)$. □

Note that Proposition 3.6 is constructive. The mapping η is determined by elements x and g, and by an integer t. If both x and g are of finite order, then $t^{|x|} \equiv 1 \bmod |g|$ holds in both cases (B) and (C). (The case $t = -1$ is stated separately only because it allows for an infinite order of g.) Note that from $t^{|x|} \equiv 1 \bmod |g|$ it immediately follows that t is coprime to $|g|$.

4. The loop operation

Let $H = H(+)$ be a cyclic group generated by an element a, and let $K = K(+)$ be generated by x. Let Q be the loop $S(H, K, \gamma)$, where $\gamma : H \to \operatorname{Aut} K$, $\gamma_{jx} = \gamma(jx)$, and $\gamma(0) = \mathrm{id}_H$. Let Γ be the subgroup of $\operatorname{Aut} H$ that is generated by $\operatorname{Im}\gamma$, and let D be the subgroup of H^K generated by all mappings $d(jx, ha) : ix \mapsto \gamma_{(i+j)x}(ha) - \gamma_{jx}(ha)$, where $i, j, h \in \mathbb{Z}$. To get D it suffices to consider only the case $h = 1$ since $d(jx, ha) = hd(jx, a)$. We know, by Corollary 1.7, that $\operatorname{Inn} Q$ is isomorphic to a semidirect product of D and Γ.

We shall be assuming throughout this section that D is *cyclic*. This assumption is justified by Corollary 2.9. However, not all loops with D cyclic have to fulfil the hypothesis of Corollary 2.9. Our main emphasis will be upon the case $Z(Q) = 1$.

From Lemma 3.1 we know that the mapping $\eta : K \times K \to H$, $(ix, jx) \mapsto \gamma_{(i+j)(x)}(a) - \gamma_{ix}(a)$ fulfils the the assumptions of Proposition 3.6. By setting $i = 0$ we obtain $\gamma_{jx}(a) = a + \eta(0, jx)$. Furthermore, $g = \eta(0, x)$ is a multiple of a, say $g = sa$. From Proposition 3.6 we thus get immediately the following statement:

Lemma 4.1. *Under the assumptions above, there exists $s \in \mathbb{Z}$ such that for all $j \in \mathbb{Z}$*

(i) *either $\gamma_{jx}(a) = (1 + js)a$ and there exists a homomorphism $K \to H$ with $x \mapsto sa$,*

(ii) *or there exist $t, t' \in \mathbb{Z}$ such that $sa = t'tsa$, $sa \neq tsa$ and*

$$\gamma_{jx}(a) = (1 + s\frac{t^j - 1}{t - 1})a.$$

Proposition 4.2. *Let $Q = S(H, K, \gamma)$, where $H = H(+)$ is generated by a, and $K = K(+)$ is generated by x, $\gamma_0 = \mathrm{id}_H$. Suppose that the mappings $ix \mapsto \gamma_{(i+j)x}(a) - \gamma_{jx}(a)$, where $i, j \in \mathbb{Z}$, generate a cyclic subgroup of H^K. If H is infinite, then Q has to be a group.*

Suppose that H is of a finite order $m > 1$ and that $Z(Q) = 1$. Then there exist $s, t \in \mathbb{Z}_m^*$ such that $t - 1 \in \mathbb{Z}_m^*$, $k = |x| = |K|$ coincides with the order of t in $\mathbb{Z}_m^*$, and

$$\gamma_{jx}(a) = (1 - s + st^j)a \text{ for all } j \in \mathbb{Z}.$$

Proof. Suppose first that H is infinite. If $s \neq 0$, then case (i) of Lemma 4.1 does not apply since there can be at most two values j for which there exists an automorphism of H that sends a to $(1 + js)a$. From Proposition 3.6 we know that $t = -1$ can be assumed, and so only the case $j = 1$ requires our attention. We have $\gamma_x(a) = a + sa$, which yields $s \in \{0, -2\}$. If $s = 0$, then $Q \cong H \times K$. If $s = -2$, then γ_x maps a to $-a$, and we get the infinite dihedral group.

Let H be of a finite order $m > 1$. Assume first that $(s, m) > 1$. Then there exists $i \in \mathbb{Z}$ such that $ia \neq 0$ and $sia = 0$. In both cases of Lemma 4.1 we get $\gamma_{jx}(ia) = ia$, for all $j \in \mathbb{Z}$. Thus $ia \in H_\zeta$ and $Z(Q) \neq 1$, by Lemma 2.3. Therefore $(s, m) = 1$ and there exists $s' \in \mathbb{Z}$ with $ss' \equiv 1 \bmod m$. In case (i) of Lemma 4.1 we get $\gamma_{-s'x} = 0$. That contradicts the assumption that $\gamma_{jx} \in \operatorname{Aut} H$ for all $j \in \mathbb{Z}$.

We can hence turn to case (ii) of Lemma 4.1. Our first goal is to prove that $t - 1$ is invertible modulo m. If it is not so, then there exists $c \in H$, $c \neq 0$, such that $(t - 1)c = 0$. In other words $t^i c = c$ for all $i > 0$. For every $j > 0$ we thus get $\gamma_{jx}(c) = (1 + s(1 + t + \cdots + t^{j-1}))c = (1 + sj)c$. Setting $j = -s'$ brings a contradiction similar to that of case (i) since $\gamma_{-s'x}(c) = 0$.

From Proposition 3.6 we know that $t \in \mathbb{Z}_m^*$ since we have already proved that a and $g = sa$ are of the same order m. Suppose that K is finite of order $k = |x|$. Then $t^k \equiv 1 \bmod m$, by Proposition 3.6. Consider $i \in \mathbb{Z}$ such that $0 < i < k$ and $t^i \equiv 1 \bmod m$. Then $\gamma_{ix} = \gamma_{(j+i)x}$ for all $j \in \mathbb{Z}$, and $ix \neq 0$ is a nontrivial element of K_ζ. That means $Z(Q) \neq 1$, by Lemma 2.3, contrary to our assumptions. We see that the multiplicative order of t modulo m has to be exactly k. If K is infinite, then K_ζ is surely notrivial since it contains all ix for which $t^i \equiv 1 \bmod m$.

It remains to replace s in the formula of Lemma 4.1 with $s(t - 1)^{-1}$. □

Note that we did not exclude the existence of $Q = S(H, K, \gamma)$ that would correspond to case (i) of Lemma 4.1. We only proved that this case does not take place if $Z(Q) = 1$.

Note also that the existence of the required s and t does not guarantee the existence of a loop $Q = S(H, K, \gamma)$. For the loop to exist all integers $1 - s + st^j$, $j \geq 0$, have to be coprime to m. However, if they are, then the mappings γ_{jx} are automorphisms of H, the loop Q is well defined, and $d(jx, a)$ sends ix to $st^j(t^i - 1)a$. That means that in such a case D is indeed cyclic. It is generated by the mapping $ix \mapsto (t^i - 1)a$ since $ss' \equiv 1 \bmod m$ for some $s' > 0$.

We shall prove that the loop of Proposition 4.2 does not depend on the choice of t, but only on the subgroup generated by t. We shall use the following general assertion.

Lemma 4.3. *Let H and K be groups, and let $\gamma : K \to \operatorname{Aut} H$ be a mapping, $\gamma_1 = \mathrm{id}_H$. Then for every $\alpha \in \operatorname{Aut} K$ there exists an isomorphism*

$$S(H, K, \gamma\alpha) \cong S(H, K, \gamma) : (a, x) \mapsto (a, \alpha(x)).$$

Proof. Put $Q = S(H, K, \gamma)$, $\gamma' = \gamma\alpha$ and $Q' = S(H, K, \gamma')$. Recall that $(a, x)(b, y) = (a\gamma_x(b), xy)$ is the operation of Q. The product in Q of images of (a, x) and (b, y) is equal to $(a\gamma_{\alpha(x)}b, \alpha(x)\alpha(y)) = (a\gamma'_x(b), \alpha(xy))$, which is also the image of the product of (a, x) and (b, y) in Q'. □

Every loop described in Proposition 4.2 is obviously isomorphic to a loop on $\mathbb{Z}_m \times \mathbb{Z}_k$ with operation

$$(a, x)(b, y) = (a + (1 - s + st^x)b,\ x + y),$$

where s, t, $t-1$ and all $1-s+st^x$, $x \in \mathbb{Z}_k$, are invertible modulo m, and $t \in \mathbb{Z}_m$ is of multiplicative order k. Denote this loop by Q and let Q' be another loop in which t is replaced by a power $t' = t^r$, $(r, k) = 1$. The sets of all t^x and t'^x coincide, and hence Q' is really a loop. Denote by α the automorphism of $\mathbb{Z}_k$ that sends each x to rx. Then $(a, x) \mapsto (a, \alpha(x))$ yields an isomorphism of Q' and Q, by Lemma 4.3.

For the purposes of this paper call the above loop Q a loop of *type* $[m, k, s]$. We shall always assume that m and k are greater than 1. We can state:

Proposition 4.4. *Let Q be a loop of type $[m, k, s]$. If $\mathbb{Z}_m^*$ is a cyclic group, then the triple (m, k, s) determines the isomorphism type of Q completely.*

It is immediate from Proposition 4.2 that m has to be an odd number. Hence (m, k, s) determines the isomorphism type of Q completely whenever m is a prime power. If it is not a prime power we can use Lemma 2.4 and study the subloops induced by the primary decomposition of $\mathbb{Z}_m$. Suppose $m = \prod p_i^{h_i}$. It is easy to see that there is, up to isomorphism, only one loop of type $[m, k, s]$ such that all induced subloops are of type $[p_i^{h_i}, k, s]$.

Theorem 4.5. *Let $m > 1$ and $k > 1$ be integers, and let $s, t \in \mathbb{Z}_m^*$ be elements such that the multiplicative order of t is equal to k, with $t - 1 \in \mathbb{Z}_m^*$ and with each of $1 - s + st^x$, $x \in \mathbb{Z}_k$, also invertible modulo m. Then*

$$(a, x)(b, y) = (a + (1 - s + st^x)b,\ x + y)$$

defines an LCC loop on $\mathbb{Z}_m \times \mathbb{Z}_k$. This loop is a group if and only if $s = 1$. The left nucleus is equal to $\mathbb{Z}_m \times \{x \in \mathbb{Z}_k; (s - 1)(t^x - 1) = 0\}$, and the right nucleus to $\{a \in \mathbb{Z}_m;\ (s - 1)a = 0\} \times \mathbb{Z}_k$. The center is always trivial, and the inner mapping *group is isomorphic to the subgroup $\mathbb{Z}_m \ltimes C$ of the holomorph $\mathbb{Z}_m \ltimes \mathbb{Z}_m^*$, where $C \le \mathbb{Z}_m^*$ is generated by all elements $1 - s + st^x$, $x \in \mathbb{Z}_k$.*

Proof. Our loop can be expressed as $Q = S(\mathbb{Z}_m, \mathbb{Z}_k, \gamma)$, where γ_x means the multiplication by $1 - s + st^x$. The loop Q is left conjugacy closed, by Corollary 2.2, and hence $N_\lambda = N_\mu$. Observe that

$$(1 - s + st^x)(1 - s + st^y) - (1 - s + st^{x+y}) = s(s - 1)(t^x - 1)(t^y - 1)$$

for all $x, y \in \mathbb{Z}_k$. By Lemma 2.1, $N_\lambda = \mathbb{Z}_m \times L$, where L is formed by all $x \in Q$ such that $\gamma_{x+y} = \gamma_x\gamma_y$ for every $y \in \mathbb{Z}_k$. By choosing $y = 1$ we see that $s(s-1)(t^x-1)(t^y-1)$ equals 0 for all $y \in \mathbb{Z}_k$ if and only if $(s-1)(t^x-1) = 0$, which gives the formula for L. From Lemma 2.1 we also know that $N_\rho = R \times \mathbb{Z}_k$, where $a \in R$ if and only if $s(s-1)(t^x-1)(t^y-1)a = 0$ for all $x, y \in \mathbb{Z}_k$. This is clearly true if and only if $(s-1)a = 0$.

Assume $(a, 0) \in Z(Q)$. Then $(a, 0) \in N_\rho$, and hence $(1 - s)a = 0$. Thus $\gamma_x(a) = t^x a$, and $\gamma_1(a) = a$ if and only if $a = 0$ since $t - 1$ is invertible modulo m. From Lemma 2.3 we hence see that $(a, 0) \in Z(Q)$ if and only if $a = 0$. Furthermore, $\gamma_{x+y} = \gamma_y$ for all $y \in \mathbb{Z}_k$ if and only if $t^x = t^{x+y}$ for all $y \in \mathbb{Z}_k$, which means $x = 0$. By using Lemma 2.3 once more we thus see that the center of Q is really trivial.

From Corollary 1.7 we know that $\operatorname{Inn} Q$ is isomorphic to a semidirect product of groups $D \le \mathbb{Z}_m^{\mathbb{Z}_k}$ and $\Gamma \le \operatorname{Aut} \mathbb{Z}_m$. We have observed earlier that D is generated by the mapping $i \mapsto t^i - 1$. Denote this mapping by δ. Since $t - 1 = \delta(1)$ is assumed to be invertible modulo m, we see that D is of order m, with $\delta^a(i) = (t^i - 1)a$ for each $i \in \mathbb{Z}_k$. Now, Γ clearly coincides with all multiplications $\mu_x \in \operatorname{Aut} \mathbb{Z}_m$, where $x \in C$. From Lemma 1.5 we see that $\operatorname{Inn} Q$ is isomorphic to the group on $\{(\delta^a, \mu_x);\ (a, x) \in \mathbb{Z}_m \times C\}$, where $(\delta^a, \mu_x)(\delta^b, \mu_y) = (\delta^a\mu_x\delta^b, \mu_x\mu_y)$. That is equal to $(\delta^{a+xb}, \mu_{x+y})$ since $\mu_x\delta^b(i) = x(t^i - 1)b = (t^i - 1)(xb) = \delta^{xb}(i)$, for all $i \in \mathbb{Z}_k$. The rest is clear. □

The theorem yields the following consequence:

Corollary 4.6. *Assume, in addition, that $s - 1$ is invertible modulo m. Then k is a proper divisor of $\varphi(m) = |\mathbb{Z}_m^*|$, the left nucleus equals $\mathbb{Z}_m \times 0$ and the right nucleus equals $0 \times \mathbb{Z}_k$.*

Proof. The structure of nuclei follows from Theorem 4.5 in an immediate way. Suppose $k = \varphi(m)$. Then each element of $|\mathbb{Z}_m^*|$ can be expressed in the form st^x for some $x \in \mathbb{Z}_k$. But then $(1 - s) + (s - 1) = 0$ would be invertible modulo m, and that is an obvious contradiction. □

Theorem 4.7. *Let C be a nontrivial abelian group that acts upon $\mathbb{Z}_m$, $m > 1$, in a way that is both faithful and fixed point free. Let Q be a loop in which $N_\lambda = N_\mu$ is a normal subloop and $N = N_\lambda \cap N_\rho$ is trivial. Suppose that both N_λ and N_ρ are cyclic groups. If $Q = N_\lambda N_\rho$ and $\operatorname{Inn} Q \cong \mathbb{Z}_m \ltimes C$, then there exist integers $s, t \in \mathbb{Z}_m^*$, where $s - 1, t - 1 \in \mathbb{Z}_m^*$ as well, such that Q is isomorphic to the loop on $\mathbb{Z}_m \times \mathbb{Z}_k$, $(a, x) \cdot (b, y) = (a + (1 - s + st^x)b, x + y)$ for all $a, b \in \mathbb{Z}_m$ and $x, y \in \mathbb{Z}_k$.*

Proof. From [3, Lemma 3.5] we know that Q is of the form $S(H, K, \gamma)$, where $H \cong N_\lambda$ and $K \cong N_\rho$ are cyclic. We can thus use Corollary 2.9 to obtain the cyclicity of D. The rest follows from Proposition 4.2 and Theorem 4.5 since $Z(Q) \le N_\lambda \cap N_\rho = 1$. □

The hypothesis of Theorem 4.7 is satisfied when C is a cyclic group of order n and $(n,m)=1$, by Lemma 2.8. This is, amongst others, the case of $|\operatorname{Inn} Q| = pq$.

From here on we shall usually assume that $s-1$ is invertible modulo m.

Lemma 4.8. *Let H and K be groups, and let $\gamma : K \to \operatorname{Aut} H$ be a mapping, $\gamma_1 = \mathrm{id}_H$. Then for every $\alpha \in \operatorname{Aut} H$ such that $\alpha\gamma_x = \gamma_x\alpha$ for all $x \in K$ there exists an automorphism $(a,x) \mapsto (\alpha(a),x)$ of $Q = S(H,K,\gamma)$.*

Proof. We see immediately that $(\alpha(a),x)\cdot(\alpha(b),y)$ is equal to $(\alpha(a)\gamma_x\alpha(b),xy) = (\alpha(a\gamma_x(b)),xy)$. □

Theorem 4.9. *Let $m > 1$ and $k > 1$ be integers. For $i = \{1,2\}$ let $s_i, t_i \in \mathbb{Z}_m^*$ be such that both $s_i - 1$ and $t_i - 1$ are also invertible modulo m and the multiplicative order of t_i is equal to k. Let Q_i be the loop on $\mathbb{Z}_m \times \mathbb{Z}_k$ with operation $(a,x)(b,y) = (a + (1 - s_i + s_i t_i^x)b, x+y)$. Then $Q_1 \cong Q_2$ if and only if both $\langle t_1 \rangle = \langle t_2 \rangle$ and $s_1 = s_2$ are true.*

Proof. From Corollary 4.6 we see that any isomorphism $Q_1 \cong Q_2$ can be decomposed to an automorphism of $\mathbb{Z}_m$ and an automorphism of $\mathbb{Z}_k$. However, the latter can be assumed to be the identity, by Lemma 4.8. The rest follows from Lemma 4.3. □

5. Isotopes

Theorem 4.9 makes clear the isomorphism problem, our goal now is to clarify the relationships of isotopy. Our first statement can be verified in an immediate way.

Lemma 5.1. *Let Q a loop on $\mathbb{Z}_m \times \mathbb{Z}_k$ with operation $(a,x)(b,y) = (a + (1 - s + st^x)b,\ x+y)$. Then*

$$(a,x)/(b,y) = (a - (1 - s + s^{x-y})b,\ x-y) \text{ and}$$
$$(a,x)\backslash(b,y) = ((1 - s + st^x)^{-1}(b-a),\ y-x).$$

Let Q be a loop, $a \in Q$. The right translation R_a can be interpreted as a loop isomorphism between operations $(x \cdot ya)/a$ and $(x/a)y$. Similarly, L_b, $b \in Q$, can be used to connect operations $b\backslash(bx \cdot y)$ and $x(b\backslash y)$. To get all principal isotopes of Q it hence suffices to apply, for all $b \in Q$, one of the two latter operations upon loops obtained, for all $a \in Q$, by one of the two former operations.

If $(\beta, R_a\beta, R_a\beta)$ is an autotopism of Q, then $(\beta(x)\cdot\beta(y)a)/a = \beta(xy)$ for all $x,y \in Q$, and so the mapping β is an isomorphism between operations $(x \cdot ya)/a$ and xy. For an LCC loop Q one can find such an isomorphism β for every $a \in Q$ since $(R_a^{-1}L_a, L_a, L_a)$ is always an autotopism. The first stage of the search for loop isotopes can be thus omitted if Q is an LCC loop.

If $a \in N_\lambda$, then $(ax)\backslash y = x\backslash(a^{-1}y)$ for all $x,y \in Q$, and hence $b\backslash(bx\cdot y) = b'\backslash(b'x \cdot y)$ if $b' = ab$ for some $a \in N_\lambda$. Therefore only the elements $b \in S$ need to be considered if $Q = N_\lambda S$ for some $S \le Q$.

The loops we are studying are LCC and are products of N_λ and N_ρ, by Theorem 4.5.

Theorem 5.2. *Suppose that s,t,m,k are integers such that s, t and $t-1$ are invertible modulo m, and k is the multiplicative order of t modulo m. Let Q be a loop on $\mathbb{Z}_m \times \mathbb{Z}_k$ with operation $(a,x)(b,y) = (a+(1-s+st^x)b,\, x+y)$. For each $j \in \mathbb{Z}_k$ consider the loop on $\mathbb{Z}_m \times \mathbb{Z}_k$ with operation $(a,x)\circ(b,y) = (a+(1-s'+s't^x)b,\, x+y)$, where $s' = st^j/(1-s+st^j)$. This loop is isotopic to Q, and every loop isotopic to Q is isomorphic, for some $j \in \mathbb{Z}_k$, to such a loop. If $s-1$ is invertible modulo m, then there are, up to isomorphism, exactly k loops isotopic to Q.*

Proof. The considerations preceding the theorem imply that each loop isotopic to Q is isomorphic to an isotope with operation

$$(a,x)\circ(b,y) = (0,j)\backslash((0,j)(a,x)\cdot(b,y)) = (a + \frac{1-s+st^{j+x}}{1-s+st^j}b,\, x+y),$$

where $j \in \mathbb{Z}_k$. We have

$$\frac{1-s+st^{j+x}}{1-s+st^j} = 1 - \frac{st^j}{1-s+st^j} + \frac{st^j}{1-s+st^j}t^x,$$

and so it remains to show that if $1-s$ is invertible modulo m, then $st^j/(1-s+st^j)$ equals $st^{j'}/(1-s+st^{j'})$ if and only if $j = j'$, for all $j, j' \in \mathbb{Z}_k$. Put $\delta = j'-j$. We get $t^\delta(1-s+st^j) = 1-s+st^{j'}$, which gives $t^\delta(1-s) = 1-s$, $t^\delta = 1$, $\delta = 0$ and $j = j'$. □

6. The existence

Up to now we did not address the question for which parameters k and s does a loop of type $[m,k,s]$ exist. The decomposition procedure of Lemma 2.4 allows a reduction to the case $m = p^r$, $r \geq 1$, where p is an odd prime, by Proposition 4.2. In this section we shall consider only that case.

Let us recall that by a loop of type $[m,k,s]$ we mean here a loop on $\mathbb{Z}_m \times \mathbb{Z}_k$ with operation $(a,x)(b,y) = (a+(1-s+st^x)b,\, x+y)$, where t is of the multiplicative order k modulo m, $s \in \mathbb{Z}_m^*$ and $t-1 \in \mathbb{Z}_m^*$. Note that the latter condition means that if $m = p^r$, $k = p^{r'}k'$ and $(k',p) = 1$, then $k' \neq 1$.

The operation defines a loop if and only if $1-s+st^x \in \mathbb{Z}_{p^r}^*$ for all $x \in \mathbb{Z}$. The incidence to $\mathbb{Z}_{p^r}^*$ can be also written as $s \not\equiv 0$, $t \not\equiv 0, 1$ and $1-s+st^x \not\equiv 0 \bmod p$. That makes the following statement immediately clear.

Proposition 6.1. *Let p be an odd prime, and let $k > 1$ and $s > 1$ be integers that are not divisible by p, $k \not\equiv 1 \bmod p$. Suppose that k is an order of a subloop of $\mathbb{Z}_{p^r}^*$ and $p^r > s$. Define $k', s' \in \{1,2,\ldots,p-1\}$ and $r' \geq 1$ by $k = p^{r'}k'$ and $s' \equiv s \bmod p$. A loop of type $[p^r,k,s]$ exists if and only a loop of type $[p,k',s']$ exists.*

From here on we shall be considering only loops of type $[p,k,s]$.

Proposition 6.2. *Let p be an odd prime and k a proper divisor of $p-1$. Denote by T the k-element subgroup of $\mathbb{Z}_p^*$. A loop of type $[p,k,s]$ exists if and only if $s^{-1} \notin 1-T$. For each k there are $p-k$ possible choices for s. The choices yield pairwise nonisomorphic loops that make $(p-1)/k$ isotopism classes, one of which is formed by a group.*

Proof. There are $p-1$ choices for $s \not\equiv 0 \bmod p$. The condition $1-s+st^x \not\equiv 0$, $x \in \mathbb{Z}$, can be written as $1-s \notin -sT$, and that is equivalent to $s^{-1} \notin 1-T$. The set $1-T$ contains 0, and hence from the original $p-1$ choices of s there must be removed $k-1$ choices. If $s=1$, we get a group, by Theorem 4.5, and $s-1$ is invertible modulo p in other cases. The rest follows from Theorems 4.9 and 5.2. □

Corollary 6.3. *Let p be an odd prime and let $n > 2$ be a divisor of $p-1$. Then there exists a loop of type $[p, 2, s]$ with inner mapping group isomorphic to the subgroup $\mathbb{Z}_p \ltimes C$ of the holomorph $\mathbb{Z}_p \ltimes \mathbb{Z}_p^*$, $C \cong \mathbb{Z}_n$.*

Proof. If $k=2$, then the group T is equal to $\{-1, 1\}$, and we have to avoid the choice $s^{-1} \equiv 2 \bmod p$. Let C be the n-element subgroup of $\mathbb{Z}_p^*$. Then C contains a generator different from -1, and hence such a generator can be expressed as $1-2s = 1-s+s(-1)$, $s \notin \{0, 1, 2^{-1}\}$. By Theorem 4.5 this suffices for the sought loop to exist. □

For $k \geq 3$ it seems far more complicated to determine when there exists a loop of type $[p, k, s]$ with a prescribed inner mapping group of order $n \ll p$. However, to find examples is not difficult. We give an example for $p = 43$, $k = 3$ and $n = 7$:

Sets $T = \{1, 6, 36\}$ and $C = \{1, 4, 11, 16, 21, 35, 41\}$ form subgroups of $\mathbb{Z}_{43}^*$. A loop Q of type $[43, 3, s]$ will have $\operatorname{Inn} Q \cong \mathbb{Z}_{43} \ltimes C$ if and only if both $1-s+6s \equiv 5s+1$ and $1-s+36s \equiv 1-8s$ get into C. Choose $s = 35 \equiv -8$. Then $5s+1 = -39 \equiv 4$ and $1-8s = 65 \equiv 21 \bmod 43$.

7. Cyclicity of the right nucleus

In this section we shall make clear that the construction of this paper always applies when Q is a loop with $Z(Q) = 1$, $|\operatorname{Inn} Q| = pq$ and $Q = N_\lambda N_\rho$, where $N_\lambda = N_\mu \trianglelefteq Q$. Our departing point will be the following result based upon [2, Theorem 4.6]:

Proposition 7.1. *Let Q be a loop with $Z(Q) = 1$ and $|\operatorname{Inn} Q| = pq$, where $q < p$ are primes. Then Q contains a p-element subgroup $S \lhd Q$ such that Q/S is an abelian group of order $k \leq q$. Furthermore $|\operatorname{Mlt} Q| = p^2kq$.*

We shall now, in a series of lemmas, illuminate the structure of Q under the assumption that the initial conditions of this section are satisfied. The case of Q a group is well known, and so we shall also assume that $N_\lambda \neq N_\rho$.

By Proposition 7.1, $\operatorname{Mlt}(Q/S) \cong Q/S$ is an abelian group of order k. Hence the group $K \trianglelefteq \operatorname{Mlt} Q$ of permutations which act within the cosets modulo S is of order p^2q. The unit $1 \in Q$ is the only point fixed by $\operatorname{Inn} Q$ since $Z(Q) = 1$. Hence the image of $\operatorname{Inn} Q$ upon S has to be a q-element permutation group. The action of K upon S thus cannot be faithful. However, each L_s and R_s, $s \in S$, belongs to K. The image of K upon S is hence of order pq, and that makes the following lemma obvious.

Lemma 7.2. *The group K contains an elementary abelian subgroup normal subgroup of order p^2.*

We shall denote this sugroup by P.

Lemma 7.3. *Every nontrivial element of P fixes pointwise elements of at most one coset modulo S.*

Proof. If it fixes pointwise two different cosets, then conjugation can be used to establish the existence of a nontrivial $\varphi \in \operatorname{Inn} Q \cap P$ that fixes pointwise elements of a coset $B \neq S$. Choose $\psi \in \operatorname{Inn} Q$ of order q. Then ψ fixes an element $b \in B$. This b is thus fixed by every element of $\operatorname{Inn} Q$, and hence it belongs to $Z(Q)$. That is a contradiction. □

Lemma 7.4. *Every nontrivial normal subloop of Q contains S.*

Proof. Suppose that $b \notin S$ belongs to a normal subloop. Let B be the coset modulo S that contains b. To prove that the normal subloop contains S it suffices to show that it contains B. However, that follows from Lemma 7.3 since every element of B is equal to some $\varphi(b)$, $\varphi \in P \cap \operatorname{Inn} Q$. □

The right nucleus N_ρ coincides with the points fixed by $\mathcal{L}_1$, where $\mathcal{L} = \langle L_x;\ x \in Q\rangle$ is the *left multiplication group* of Q. Similarly, N_λ are the elements fixed pointwise by the unit stabilizer of the *right multiplication group* $\mathcal{R}$.

We assume $N_\lambda \trianglelefteq Q$, and hence Lemma 7.4 implies that $\mathcal{R}_1$ has to coincide with $P \cap \operatorname{Inn} Q$, which means $N_\lambda = S$. Furthermore, we have $N_\lambda \neq N_\rho$, and so N_ρ has to be formed by fixed points of a q-element subgroup of $\operatorname{Inn} Q$. That makes the following assertion clear.

Lemma 7.5. *The left nucleus N_λ coincides with S. The right nucleus N_ρ intersects each coset of S in exactly one point and is isomorphic to Q/S. Furthemore, $|\mathcal{L}| = pqk$ and $|\mathcal{R}| = p^2k$.*

Lemma 7.6. *The group P is formed by all mappings $L_sR_{s'}$, where $s, s' \in S$, and the group N_ρ is cyclic.*

Proof. We assume $N_\lambda = N_\mu$, and this group is known to coincide with S. Therefore, $L_sL_{s'} = L_{ss'}$ and $R_sR_{s'} = R_{s's}$ for all $s, s' \in S$. Furthermore, $R_sL_{s'} = L_{s'}R_s$, and so we see that the mappings $L_sR_{s'}$ form a group of exponent p. If $L_s = R_s$, then $s \in Z(Q) = \{1\}$, since $s \in N_\lambda \cap N_\mu$. The group thus has to be of order p^2, and so it equals P.

Now, P is a characteristic subgroup of $K \lhd \operatorname{Mlt} Q$, and therefore $P \lhd \operatorname{Mlt} Q$. Hence $\operatorname{Mlt} Q$ acts by conjugation upon P, and this action induces an action of $\operatorname{Mlt} Q$ upon the projective line formed by the 1-dimenesional subspaces of P. Restrict this action only to the action of the group $\{R_a;\ a \in N_\rho\} \cong N_\rho$. This action is faithful since no R_a, $a \neq 1$, fixes the projective point $P \cap \operatorname{Inn} Q$. However, the action fixes the projective point $\{L_s;\ s \in S\}$, and so the group can be embedded into the point stabilizer of $PSL(2, p)$ (in the natural representation on $p+1$ points). This stabilizer is a solvable group of order $p(p-1)$, and so every k-element subgroup is a subgroup of a $(p-1)$-element subgroup. These subgroups are known to be cyclic, and hence each k-element subgroup is cyclic as well. Our k-element subgroup was chosen to be isomorphic to N_ρ, and that brings us to the end of this proof. □

We see that our initial assumptions yield a situation in which one can use Theorem 4.7. We can thus conclude this section by the following theorem.

Theorem 7.7. *Let Q be a loop with $Z(Q) = 1$ and $|\operatorname{Inn} Q| = pq$, where $p > q$ are primes. Suppose that $N_\lambda = N_\mu \trianglelefteq Q$ and that $Q = N_\lambda N_\rho$. Then Q is isomorphic to a loop upon $\mathbb{Z}_p \times \mathbb{Z}_k$, where k divides $p-1$, there exist $s, t \in \mathbb{Z}_p^*$ such that t is of multiplicative order k modulo p, the set of all $1 - s + st^x$, $x \in \mathbb{Z}$, generates the*

q-element subgroup of $\mathbb{Z}_p^*$, and $(a,x)\cdot(b,y) = (a + (1-s+st^x)b,\, x+y)$, for all $a,b \in \mathbb{Z}_p$ and $x,y \in \mathbb{Z}_k$.

8. Conclusions

We have provided a construction that yields many nonassociative centerless loops Q with $\operatorname{Inn} Q$ being a subgroup of the holomorph of $\mathbb{Z}_m$, where m is an odd integer. We have also shown that the construction gets enforced in many cases when Q is assumed to be a product of N_λ and N_ρ, with $N_\lambda = N_\mu \trianglelefteq Q$. In particular this is true when $|\operatorname{Inn} Q| = pq$ and $Z(Q) = 1$. This case is the main motivation behind this study. The loops described here are of certain interest in themselves, but not to an extent that would warrant such a concentrated effort, had not they belong to a wider class that is worth investigation. This wider class consists of all loops Q with $|\operatorname{Inn} Q| = pq$ and $Z(Q) = 1$. The loops described in this paper are LCC, but not RCC. The CC (i.e. LCC + RCC) loops of this class are described in [4] (there is exactly one nonassociative loop of these properties, for every pair of primes (p,q), where q divides $p-1$). Then there is an interesting subclass of loops of the form $N_\lambda N_\mu$, in which $N_\lambda = N_\rho$ and $|N_\mu| = 2$, see [5]. Preliminary results show that there exists only one additional subclass. Properties of loops in that category are a subject of an ongoing research. Furthermore, there is some hope that the results pertaining to loops with $|\operatorname{Inn} Q| = pq$ will be transferred to a wider range of metacyclic inner mapping groups. This paper was based somewhat more broadly than required by the case pq in anticipation of such results.

References

[1] P. Csörgő and M. Niemenmaa: On connected transversals to nonabelian subgroups, *European J. Combin.* **23** (2002), 179–185.

[2] A. Drápal: Orbits of inner mapping groups, *Monatsh. Math.* **134** (2002), 191–206.

[3] A. Drápal: On left conjugacy closed loops with a nucleus of index two, *Abh. Math. Sem. Univ. Hamburg* **74** (2004), 205–221.

[4] A. Drápal: Structural interactions of conjugacy closed loops, *Trans. Amer. Math. Soc.* (in press).

[5] A. Drápal and P. Jedlička: On loop identities that can be obtained by a nuclear identification (submitted).

[6] T. Kepka and M. Niemenmaa: On loops with cyclic inner mapping groups, *Arch. Math. (Basel)* **60** (1993), 233–236

[7] K. Myllylä and M. Niemenmaa: On the solvability of commutative loops and their multiplication groups, *Comment. Math. Univ. Carolin.* **40** (1999), 209–213

[8] M. Niemenmaa: On finite loops whose inner mapping groups have small orders, *Comment. Math. Univ. Carolin.* **37** (1996), 651–654

[9] M. Niemenmaa: On connected transversals to subgroups whose order is a product of two primes, *European J. Combin.* **18** (1997), 915–919.

Dept. of Mathematics, Charles University, Sokolovská 83, 186 75 Praha 8, Czech Rep.

E-mail address: `drapal@karlin.mff.cuni.cz`