A class of commutative loops with metacyclic inner mapping groups

Aleš Drápal

Abstract. We investigate loops defined upon the product $\mathbb{Z}_m \times \mathbb{Z}_k$ by the formula $(a,i)(b,j) = ((a+b)/(1+tf^i(0)f^j(0)), i+j)$, where $f(x) = (sx+1)/(tx+1)$, for appropriate parameters $s,t \in \mathbb{Z}_m^*$. Each such loop is coupled to a 2-cocycle (in the group-theoretical sense) and this connection makes it possible to prove that the loop possesses a metacyclic inner mapping group. If $s = 1$, then the loop is an A-loop. Questions of isotopism and isomorphism are considered in detail.

Keywords: A-loop, nucleus, inner mapping group, cocycle, linear fractional

Classification: Primary 20N05; Secondary 08A052

Let $m \geq 3$ be an integer, and let the operation

$$(a,i) \cdot (b,j) = (\,(-1)^{ij}(a+b),\, i+j)$$

be defined upon $\mathbb{Z}_m \times \mathbb{Z}_2$. The operation yields a commutative loop, say Q, in which $(0,0)$ is the unit element.

The middle nucleus N_μ contains every $(b,0)$ since

$$(a,i)(b,0) \cdot (c,j) = ((-1)^{ij}(a+b+c), i+j) = (a,i) \cdot (b,0)(c,j)$$

for all $a,c \in \mathbb{Z}_m$ and $i,j \in \mathbb{Z}_2$. We also have

$$(b,0)(0,1) \cdot (0,1) = (-b,0) \;\text{ and }\; (b,0) \cdot (0,1)(0,1) = (b,0).$$

The left nucleus N_λ can thus contain $(b,0)$ only when $2b = 0$, and one easily derives that $N_\lambda = 1$ when m is odd. Furthermore, since we assume $m \geq 3$, there exists $b \in \mathbb{Z}_m$ with $2b \neq 0$. Hence $(0,1) \notin N_\mu$ and $N_\mu = \mathbb{Z}_m \times \{0\}$.

The inner mapping $L(x,y) = L_{xy}^{-1}L_xL_y$ is always trivial when $y \in N_\mu$. To characterize all inner mappings of Q it thus suffices to assume $x = (a,i)$ and $y = (b,1)$. We obtain mappings

$$(c,0) \mapsto ((-1)^i c, 0), \quad (c,1) \mapsto ((-1)^i(c-2a), 1),$$

Work supported by Institutional Grant MSM 0021620839.

and hence $\operatorname{Inn} Q$, the inner mapping group, is isomorphic to the dihedral group D_{2m}.

The purpose of this paper is to introduce a class of loops that can be regarded as a generalization of this initial example. We shall be constructing loops Q in which $N_\mu \trianglelefteq Q$ is a cyclic group of order m, Q/N_μ is a cyclic group of order k, $N_\lambda = N_\rho = 1$, and the inner mapping group $\operatorname{Inn} Q$ is metacyclic of order mk (and embeds into the holomorph $\mathbb{Z}_m \ltimes \mathbb{Z}_m^*$).

These loops are defined by formula

$$(a, i) \cdot (b, j) = \left(\frac{a + b}{1 + tf^i(0)f^j(0)}, i + j\right),$$

where $f : x \mapsto (sx + 1)/(tx + 1)$ is an appropriate linear fractional mapping.

This formula was discovered while studying loops Q with $|\operatorname{Inn} Q| = pq$, where $q < p$ are primes. Such loops were first investigated by Niemenmaa et al. in a series of papers [12], [13], [11], [4], [5]. The goal was to show that such loops are always solvable. That was proved in [6], where there were also established several structural properties of such loops.

It seems to be possible to exactly describe all *centerless* loops Q with $|\operatorname{Inn} Q| = pq$. They form several classes, three of which have already obtained a detailed attention [7], [8], [9]. This paper discusses a fourth class. Preliminary calculations indicate that this class contains, up to isotopy, all commutative cases, and that there exist only two further classes.

In the future one can hope to obtain similar results for all centerless loops with a metacyclic inner mapping group. That is the main reason why in this paper we do not restrict our attention to the cases $m = p$ and $k = q$ which are presently the most relevant.

To connect the general formula with our initial example, set $s = -1$ and $t = -2$. Then $f(0) = 1$, $f(1) = 0$, and $(1 - 2f(0)f(0))^{-1} = -1$.

Section 1 presents the key technical result that associates a linear fractional mapping f with a group-theoretical 2-cocycle. In Section 2 we introduce a general loop construction that depends upon a cocycle $\vartheta : G \times G \to R^*$, where R is a commutative ring, and derive some basic properties of this construction. In Section 3 we start to investigate loops with operations determined by a linear fractional mapping. The formula will be used not only for $\mathbb{Z}_m$, but for any module M over a commutative ring R. In this broader setting the linear fractional mapping $f : x \mapsto (sx{+}1)/(tx{+}1)$, $x \in R$, is assumed to be such that $1{+}tf^i(0)f^j(0)$ is an invertible element in R for all $i, j \in \mathbb{Z}$. The cocycle identity is then used to show that many required properties of $\operatorname{Inn} Q$ are true under these more general assumptions as well.

In Section 4 we explain when different linear fractional mappings yield isomorphic loops, and in Sections 5 and 6 we pay attention to the questions of isotopism.

Section 7 then reiterates the main results for the case when $R = \mathbb{Z}_m$. In this section we also explain why it is easy to construct examples of the investigated loops.

If $s = 1$, then the constructed commutative loops are A-loops, i.e. the loops in which every inner mapping is an automorphism (Theorem 3.6). A-loops were first studied by Bruck and Paige [3]. Diassociative A-loops are Moufang, by Kinyon, Kunen and Phillips [10]. It is not known if there exists a nonassociative finite simple A-loop. In fact, it seems difficult to construct a nontrivial finite A-loop with a trivial middle nucleus. Our loops are commutative, but not diassociative, and the factor over the middle nucleus is associative.

1. Cocycles and fractional mappings

Let R be a commutative ring and let f be a partial mapping $R \to R$. We shall say that f is 0-*bijective* if

(i) $f^i(0)$ is defined for each $i \geq 1$;
(ii) for each $i \geq 1$ there exists a unique $y \in R$ such that $f^i(y)$ is defined and equal to 0; and
(iii) $f(0) \in R^*$.

A partial mapping $f : R \to R$ is said to be *fractional linear* if there exist $a, b, c, d \in R$ such that $ad - bc \in R^*$ and $f : x \mapsto (ax + b)/(cx + d)$. The mapping f is regarded as defined at $x \in R$ exactly when $cx + d \in R^*$. (There are obviously more general ways to express that a fraction yields an element of R. They may turn out to be useful in future.)

Lemma 1.1. *Let f be a (partial) linear fractional mapping $R \to R$. Then f is injective. If f is 0-bijective, then f^{-1} is a 0-bijective linear fractional mapping as well, and there exist $a, b \in R^*$ and $c \in R$ such that $f(x) = (ax + b)/(cx + 1)$ whenever f is defined at x. The inverse mapping can be expressed as $x \mapsto (-x + b)/(cx - a)$.*

PROOF: We assume that $f(x)$, when defined, is equal to $(ax + b)/(cx + d)$, where $ad - bc \in R^*$. If $f(x) = f(y)$, then $(ax + b)(cy + d) = (ay + b)(cx + d)$, $(ad - bc)(x - y) = 0$ and $x = y$. Hence f has to be injective.

We have $f(0) = b/d$, and so $d \in R^*$, since f is assumed to be defined at 0. Thus (a, b, c, d) can be replaced by $(ad^{-1}, bd^{-1}, cd^{-1}, 1)$ and we can assume $d = 1$. Then $b = f(0) \in R^*$, by the definition of a 0-bijective mapping. There also has to exist $x \in R$ with $f(x) = 0$, and we see that this takes place if and only if $ax + b = 0$ and $cx + 1 \in R^*$. Now, $ax + b = 0$ and $b \in R^*$ yield $a \in R^*$.

Let us turn our attention to the inverse mapping. The equality $y = (ax + b)/(cx + d)$ is completely equivalent to $x = (-dy + b)/(cy - a)$ only when both $cx + d$ and $cy - a$ belong to R^*. If this is true for $cx + d$, then we get

$$cy - a = c\frac{ax + b}{cx + d} - \frac{acx + ad}{cx + d} = \frac{cb - ad}{cx + d} \in R^*,$$

and one can proceed in the converse direction as well. We see that the mapping $x \mapsto (-dx+a)/(cx-a)$ realizes the inverse of f, and is also 0-bijective. $\square$

Fix now a 0-bijective fractional linear mapping $f : x \mapsto (ax+b)/(cx+1)$. We shall write $\gamma(i)$ as a shortcut for $f^i(0)$, $i \in \mathbb{Z}$.

Lemma 1.2. *The element $b + c\gamma(i)\gamma(j)$ belongs to R^* for all $i, j \in \mathbb{Z}$, and*

$$\gamma(i+j) = \frac{b\gamma(i) + b\gamma(j) + (a-1)\gamma(i)\gamma(j)}{b + c\gamma(i)\gamma(j)}\,.$$

Proof: For $j = 0$ the statement reduces to $b \in R^*$ and $\gamma(i) = (b\gamma(i))/b$, which is clearly true. We shall proceed by induction on $j \geq 0$.

By the definition of γ and by the induction assumption,

$$\begin{aligned}\gamma(i+j+1) &= \frac{a\gamma(i+j)+b}{c\gamma(i+j)+1}\\ &= \frac{ab\gamma(i) + ab\gamma(j) + (a^2-a)\gamma(i)\gamma(j) + b^2 + bc\gamma(i)\gamma(j)}{cb\gamma(i) + cb\gamma(j) + (ac-c)\gamma(i)\gamma(j) + b + c\gamma(i)\gamma(j)}\,,\end{aligned}$$

where the denominator belongs to R^*. We also have $c\gamma(j)+1 \in R^*$, and hence the fraction can be also written as

$$\begin{aligned}&\frac{b\gamma(i)(c\gamma(j)+1) + (a\gamma(j)+b)(b+(a-1)\gamma(i))}{b(c\gamma(j)+1) + \gamma(i)c(a\gamma(j)+b)}\\ &\quad= \frac{b\gamma(i) + \frac{a\gamma(j)+b}{c\gamma(j)+1}(b+(a-1)\gamma(i))}{b + \frac{a\gamma(j)+b}{c\gamma(j)+1}\gamma(i)c} = \frac{b\gamma(i) + b\gamma(j+1) + (a-1)\gamma(i)\gamma(j+1)}{b + c\gamma(i)\gamma(j+1)}\,,\end{aligned}$$

where all of the denominators belong to R^*.

For $j \leq 0$ one can use the mapping $g(x) = f^{-1}(x) = (a^{-1}x - a^{-1}b)/(a^{-1}c+1)$, by Lemma 1.1. The preceding part of the proof yields

$$\begin{aligned}\gamma(i+j) = g^{-i-j}(0) &= \frac{-a^{-1}bg^{-i}(0) - a^{-1}bg^{-j}(0) + (a^{-1}-1)g^{-i}(0)g^{-j}(0)}{-a^{-1}b - a^{-1}cg^{-i}(0)g^{-j}(0)}\\ &= \frac{b\gamma(i) + b\gamma(j) + (a-1)\gamma(i)\gamma(j)}{b + c\gamma(i)\gamma(j)}\,,\end{aligned}$$

for all $j \leq 0$ and $i \in \mathbb{Z}$, and hence the statement holds for all $i, j \in \mathbb{Z}$. $\square$

Lemma 1.3. *For all $i,j,k\in\mathbb{Z}$*

$$\begin{aligned}&c\gamma(i+j)\gamma(i)\gamma(j)\gamma(k)+b\gamma(i)\gamma(j)+b\gamma(i+j)\gamma(k)\\&\qquad\qquad=c\gamma(i)\gamma(j)\gamma(k)\gamma(j+k)+b\gamma(j)\gamma(k)+b\gamma(i)\gamma(j+k).\end{aligned}$$

PROOF: We shall proceed by induction on $k\geq 0$. The case $k=0$ is clear. The induction step rests in proving $A_1(i,j,k)=0$ under the assumption that the equality holds for i, j and k, where

$$\begin{aligned}A_1(i,j,k)=\;&c\gamma(i+j)\gamma(i)\gamma(j)\gamma(k+1)\\&+b\gamma(i)\gamma(j)+b\gamma(i+j)\gamma(k+1)\\&-c\gamma(i)\gamma(j)\gamma(k+1)\gamma(j+k+1)\\&-b\gamma(j)\gamma(k+1)-b\gamma(i)\gamma(j+k+1).\end{aligned}$$

Substitute

$$\gamma(k+1)=\frac{a\gamma(k)+b}{c\gamma(k)+1}\quad\text{and}\quad\gamma(j+k+1)=\frac{a\gamma(j+k)+b}{c\gamma(j+k)+1},$$

and multiply $A_1(i,j,k)$ by the product of $c\gamma(k)+1$ and $c\gamma(j+k)+1$. The condition $A_1(i,j,k)=0$ is then equivalent to $A_2(i,j,k)=0$, where

$$\begin{aligned}A_2(i,j,k)=\;&c\gamma(i+j)\gamma(i)\gamma(j)(a\gamma(k)+b)(c\gamma(j+k)+1)\\&+b\gamma(i)\gamma(j)(c\gamma(k)+1)(c\gamma(j+k)+1)\\&+b\gamma(i+j)(a\gamma(k)+b)(c\gamma(j+k)+1)\\&-c\gamma(i)\gamma(j)(a\gamma(k)+b)(a\gamma(j+k)+b)\\&-b\gamma(j)(a\gamma(k)+b)(c\gamma(j+k)+1)\\&-b\gamma(i)(c\gamma(k)+1)(a\gamma(j+k)+b).\end{aligned}$$

Express now $A_2(i,j,k)$ as $aA_3(i,j,k)+bA_4(i,j,k)$ in such a way that $A_4(i,j,k)$ has no term containing the parameter a. Then

$$\begin{aligned}A_3(i,j,k)=\;&c\gamma(i+j)\gamma(i)\gamma(j)\gamma(k)+b\gamma(i+j)\gamma(k)-b\gamma(j)\gamma(k)-b\gamma(i)\gamma(j+k)\\&+c\gamma(j+k)\left(c\gamma(i+j)\gamma(i)\gamma(j)\gamma(k)+b\gamma(i+j)\gamma(k)-b\gamma(j)\gamma(k)\right)\\&-bc\gamma(i)\left(\gamma(j)\gamma(j+k)+\gamma(j)\gamma(k)+\gamma(k)\gamma(j+k)\right)\\&-ac\gamma(i)\gamma(j)\gamma(k)\gamma(j+k)=\;\text{(by the induction assumption)}\\=\;&c\gamma(i)\gamma(j)\gamma(k)\gamma(j+k)-b\gamma(i)\gamma(j)\\&+c\gamma(j+k)\left(c\gamma(i)\gamma(j)\gamma(k)\gamma(j+k)+b\gamma(i)\gamma(j+k)-b\gamma(i)\gamma(j)\right)\\&-bc\gamma(i)\left(\gamma(j)\gamma(j+k)+\gamma(j)\gamma(k)+\gamma(k)\gamma(j+k)\right)\end{aligned}$$

$$- ac\gamma(i)\gamma(j)\gamma(j+k)\gamma(k).$$

We can thus write $A_3(i,j,k)$ as $\gamma(i)A_5(i,j,k)$, where

$$\begin{aligned} A_5(i,j,k) = {} & \gamma(j+k)(b+c\gamma(j)\gamma(k)) - b\gamma(j+k) - b\gamma(j) \\ & + c(\gamma(j+k))^2(b+c\gamma(j)\gamma(k)) \\ & - bc\,(2\gamma(j+k)\gamma(j) + \gamma(k)\gamma(j+k) + \gamma(j)\gamma(k)) \\ & - ac\gamma(j)\gamma(j+k)\gamma(k). \end{aligned}$$

Replacing $\gamma(j+k)(b+c\gamma(j)\gamma(k))$ with $b\gamma(j) + b\gamma(k) + a\gamma(j)\gamma(k) - \gamma(j)\gamma(k)$ is possible by Lemma 1.2. By doing so we get

$$\begin{aligned} A_5(i,j,k) = {} & b\gamma(k) + a\gamma(j)\gamma(k) - \gamma(j)\gamma(k) - b\gamma(j+k) \\ & + c\gamma(j+k)(b\gamma(j) + b\gamma(k) - \gamma(j)\gamma(k)) \\ & - bc\,(2\gamma(j)\gamma(j+k) + \gamma(k)\gamma(j+k) + \gamma(j)\gamma(k)) \\ = {} & b\gamma(k) + a\gamma(k)\gamma(j) - \gamma(k)\gamma(j) - \gamma(j+k)(b+c\gamma(j)\gamma(k)) \\ & - bc\gamma(j)\gamma(j+k) - bc\gamma(j)\gamma(k) \\ = {} & \gamma(k)(b+(a-1)\gamma(j)) - b\gamma(j) - b\gamma(k) + (1-a)\gamma(j)\gamma(k) \\ & - bc\gamma(j)(\gamma(j+k)+\gamma(k)) \\ = {} & -b\gamma(j)(1+c(\gamma(j+k)+\gamma(k))). \end{aligned}$$

Thus $aA_3(i,j,k) = -ab\gamma(i)\gamma(j)(1+c(\gamma(k)+\gamma(j+k)))$, while $A_4(i,j,k)$ is equal to

$$\begin{aligned} (c\gamma(i+j)\gamma(i)\gamma(j) + c\gamma(i)\gamma(j)\gamma(k) + \gamma(i)\gamma(j) + b\gamma(i+j) - b\gamma(j)) \cdot (1 + c\gamma(j+k)) \\ - b\gamma(i)(c\gamma(k)+1) - bc\gamma(i)\gamma(j). \end{aligned}$$

We have $c\gamma(i+j)\gamma(i)\gamma(j) + b\gamma(i+j) = b\gamma(i) + b\gamma(j) + a\gamma(i)\gamma(j) - \gamma(i)\gamma(j)$, by Lemma 1.2. Hence $A_4(i,j,k) = \gamma(i)A_6(i,j,k)$, where

$$\begin{aligned} A_6(i,j,k) = {} & (1+c\gamma(j+k)) \cdot (c\gamma(j)\gamma(k) + b + a\gamma(j)) \\ & - bc\gamma(k) - b - bc\gamma(j) \\ = {} & c\gamma(j+k)(c\gamma(j)\gamma(k)+b) \\ & + c\gamma(j+k)a\gamma(j) + c\gamma(j)\gamma(k) + a\gamma(j) - bc\gamma(j) - bc\gamma(k). \end{aligned}$$

Setting $\gamma(j+k)(c\gamma(j)\gamma(k)+b) = b\gamma(j) + b\gamma(k) + a\gamma(j)\gamma(k) - \gamma(j)\gamma(k)$ yields

$$A_6(i,j,k) = a\gamma(j)(1+c(\gamma(k)+\gamma(j+k))).$$

Therefore $A_2(i,j,k) = aA_3(i,j,k) + b\gamma(i)A_6(i,j,k) = 0$. This finishes the induction step. We have proved that the equality of the lemma holds for all $i, j \in \mathbb{Z}$ and all $k \geq 0$.

For such integers the equality also holds when the mapping $\gamma : h \mapsto f^h(0)$ is replaced by the mapping $h \mapsto f^{-h}(0)$, by Lemma 1.1, and that allows an easy verification of the case $k < 0$. □

We shall be considering group-theoretical cocycles only for the case of central extensions. If H and G are groups, with H being commutative, then all 2-cocycles form the group $\Gamma^2(G,H)$, where $\sigma : G \times G \to H$ belongs to $\Gamma^2(G,H)$ if $\sigma(x,1) = \sigma(1,x) = 1$ for all $x \in G$ and if the equality $\sigma(x,y)\sigma(xy,z) = \sigma(x,yz)\sigma(y,z)$ holds for all $x, y, z \in G$. We shall be often working with the case when G is an abelian group with the operation written additively. The cocycle identity then takes the form

$$\sigma(x,y)\sigma(x+y,z) = \sigma(x,y+z)\sigma(y,z).$$

The cocycle σ is said to be *commutative* if $\sigma(x,y) = \sigma(y,x)$ for all $x, y \in G$.

Proposition 1.4. *Let R be a commutative ring and let f be a 0-bijective linear fractional mapping $R \to R$, $f(x) = (ax+b)/(cx+1)$. For all $i, j \in \mathbb{Z}$ put*

$$\sigma(i,j) = \frac{c}{b} f^i(0) f^j(0) + 1.$$

Then $\sigma \in \Gamma^2(\mathbb{Z}, R^*)$ is a commutative 2-cocycle.

Proof: Clearly, $\sigma(0,i) = \sigma(i,0) = 1$ for all $i \in \mathbb{Z}$. To verify the cocycle identity (with i, j, k in place of x, y, z) it suffices to verify the same equality for $\sigma'(i,j) = b + c\gamma(i)\gamma(j) = b\sigma(i,j)$. Define $\lambda(i,j,k)$ and $\rho(i,j,k)$ by $\sigma'(i,j)\sigma'(i+j,k) = (b + c\gamma(i)\gamma(j))(b + c\gamma(i+j)\gamma(k)) = b^2 + c\lambda(i,j,k)$ and $\sigma'(i,j+k)\sigma'(j,k) = (b + c\gamma(i)\gamma(j+k))(b + c\gamma(j)\gamma(k)) = b^2 + c\rho(i,j,k)$. It is easy to see that $\lambda(i,j,k)$ and $\rho(i,j,k)$ are in fact shortcuts for the left and right hand sides in the equality of Lemma 1.3. Hence $\lambda(i,j,k) = \rho(i,j,k)$, and nothing more is needed. □

If $f : x \mapsto (ax+b)/(cx+d)$ is a 0-bijective linear fractional mapping $R \to R$, then we can assume $d = 1$, by Lemma 1.1. We shall now observe that in fact it suffices to investigate mappings f with $b = d = 1$.

Lemma 1.5. *Let R be a commutative ring and let f be a 0-bijective linear fractional mapping $R \to R$, $f(x) = (ax+b)/(cx+1)$. Set $g(x) = (ax+1)/(bcx+1)$. Then g is a 0-bijective linear fractional mapping as well, and $f^i(0) = bg^i(0)$ for all $i \in \mathbb{Z}$.*

Proof: For $i = 0$ there is nothing to solve. Assume $f^i(0) = bg^i(0)$, where $i \geq 0$. Then

$$bg^{i+1}(0) = \frac{abg^i(0) + b}{cbg^i(0) + 1} = \frac{af^i(0) + b}{cf^i(0) + 1} = f^{i+1}(0).$$

To get the equality for $i < 0$ one can consider the inverse mapping. The rest is clear. $\square$

Similar effects can be achieved when $f(x)$ is replaced by $(ab^{-1}x+1)/(cx+1)$. The referee pointed out that this fractional mapping can be used in all instances in place of the mapping $g(x)$ from Lemma 1.5 and that working with this mapping is conceptually easier. This is true — the preference given to $g(x)$ is based only upon the fact that the definition of $g(x)$ does not require inverse elements in coefficients, which might be useful in the future.

2. Loops from cocycles

Some calculations are more transparent when done in an adequately general environment, and that is the reason why we start from a construction that involves only the notion of cocycle. Proposition 1.4 gives the reason why the main construction of this paper can be regarded as a special case.

Proposition 2.1. *Let M be a (left) module over a commutative ring R and let $G(\cdot)$ be a group. Suppose that $\vartheta \in \Gamma^2(G, R^*)$ is a 2-cocycle. Define a loop $Q = [M, G, \vartheta]$ on $M \times G$ by*

$$(a, g) \cdot (b, h) = (\vartheta(g, h)(a + b), gh).$$

Put $\varphi = L(x, y)$, where $x = (a, g)$ and $y = (b, h)$. Then

$$\varphi : (c, k) \mapsto \Big(\vartheta(g, h)\,\Big((\vartheta(h, k)^{-1} - 1)a + c\Big)\,,\, k\Big)$$

for all $(c, k) \in M \times G$. Furthermore, every $(b, 0)$ belongs to the middle nucleus.

Proof: We have $(a, g)\cdot(b, h)(c, k) = (\vartheta(g, hk)a + \vartheta(g, hk)\vartheta(h, k)b + \vartheta(g, hk)\vartheta(h, k)c, ghk)$, while

$$(\vartheta(g, h)(a + b), gh) \cdot (\vartheta(g, h)((\vartheta(h, k)^{-1} - 1)a + c), k) = (x, gh),$$

where $x = \vartheta(g, h)\vartheta(gh, k)(a + b + (\vartheta(h, k)^{-1} - 1)a + c) = \vartheta(g, hk)\vartheta(h, k)(b + c + \vartheta(h, k)^{-1}a)$. This verifies the formula for φ. If $h = 0$, then $\vartheta(g, h) = \vartheta(h, k) = 1$, φ is trivial, and $(b, 0) \in N_\mu$. $\square$

We shall be investigating loops $Q = [M, G, \vartheta]$ introduced by Proposition 2.1 for the rest of this section. The meaning of R, M, G, ϑ will be always the same as in the proposition.

In loops $xy = 1$ does not necessarily imply $yx = 1$. We write $y = x^{-1}$ only when both $yx = 1$ and $xy = 1$ are true.

Lemma 2.2. *If $x = (a, g) \in Q$, then $x^{-1} = (-a, g^{-1})$ and $x \cdot xx = xx \cdot x$. On the other hand, $xx \cdot x^{-1} = x$ if an only if $2a = (\vartheta(g, g^{-1})^{-1} + \vartheta(g, g)^{-1})a$.*

Proof: Set $\varphi = L(x, x)$. Our task is to investigate the equalities $\varphi(x) = x$ and $\varphi(x^{-1}) = x^{-1}$. From Proposition 2.1 we know that φ maps each $z = (c, k)$ to (d, k), where $d = \vartheta(g, g)((\vartheta(g, k)^{-1} - 1)a + c)$. We obtain $d = a$ if $z = (a, g)$, and $d = \vartheta(g, g)(\vartheta(g, g^{-1})^{-1} - 2)a$ if $z = (-a, g^{-1})$. □

A loop element is said to be *power associative* if the subloop generated by this element is associative (i.e. it is a group). The equality $x \cdot xx = xx \cdot x$ implies power-associativity of x in some classes of loops, but not generally. We see that Lemma 2.2 provides a plenty of examples for the general behaviour.

Lemma 2.3. *Let A be a submodule of M. Define an equivalence on Q by*

$$(a, g) \sim_A (b, h) \;\Leftrightarrow\; a - b \in A \;\text{ and }\; g = h.$$

Put $\bar{M} = M/A$, and suppose that $a \mapsto \bar{a}$ denotes the natural projection $M \to \bar{M}$. Then $(\bar{a}, g)(\bar{b}, h) = (\vartheta(g, h)(\bar{a} + \bar{b}), gh)$ defines a loop $\bar{Q}$ upon $\bar{M} \times G$, and $(a, g) \mapsto (\bar{a}, g)$ yields a surjective homomorphism $Q \to \bar{Q}$. The equivalence $\sim_A$ is equal to the kernel of this homomorphism.

Proof: Indeed, $\bar{Q}$ fulfils the assumptions of Proposition 2.1, and so it forms a loop. The rest is also easy. □

Let S be the subring of R generated (as a ring) by all $\vartheta(g, h)$. We can, clearly, regard ϑ as an element of $\Gamma^2(G, S^*)$. Hence R can be always replaced by S, whenever needed.

Let I be the ideal of R that annihilates M. The restriction of the natural projection $R \to R/I$ to R^* yields a group isomorphism $R^* \cong (R/I)^*$, and hence ϑ can be regarded as an element of $\Gamma^2(G, (R/I)^*)$. Thus R can be always replaced by R/I, and we can restrict our attention, when needed, only to faithful modules. Note however that a factorization as in Lemma 2.3 can change a faithful module to a module with nontrivial annihilator.

Proposition 2.4. *Suppose that R is generated (as a ring) by all $\vartheta(g, h)$, where $g, h \in G$. Then $A \mapsto A \times 1$ gives a one-to-one correspondence between the submodules of M and those normal subloops of $Q = [M, G, \vartheta]$ that are contained in $M \times 1$.*

Proof: The route from a submodule to a normal subloop follows from Lemma 2.3. For the other direction consider a normal subloop $P \trianglelefteq Q$, $P = A \times 1$ for some $A \subseteq M$. It is clear that $A(+)$ is a subgroup of $M(+)$. Since $A \times 1$ is normal in Q, it has to remain invariant under the permutations $L(x, y)$. That means, by Proposition 2.1, that $\vartheta(g, h)a = a$ for all $a \in A$ and $g, h \in G$. In other words, A has to be a submodule of M. □

Proposition 2.5. *Put* $T_\rho = \{g \in G;\ \vartheta(h,g)a = a$ *for all* $(a,h) \in M \times G\}$, $T_\lambda = \{g \in G;\ \vartheta(g,h)a = a$ *for all* $(a,h) \in M \times G\}$, *and* $A = \{a \in M;\ \vartheta(g,h)a = a$ *for all* $g,h \in G\}$. *Then* $N_\lambda = A \times T_\lambda$, $N_\rho = A \times T_\rho$ *and* $N_\mu = M \times (T_\lambda \cap T_\rho)$.

Proof: Choose $x, y, z \in Q$ in such a way that $x = (a,g)$, $y = (b,h)$ and $z = (c,k)$. We shall use the formula for $L(x,y)$ from Proposition 2.1.

The element y belongs to N_μ if and only if $L(x,y) = \mathrm{id}_Q$ for all $x \in Q$. This can be reduced to $(\vartheta(h,k)^{-1} - 1)a = 0$ for all $a \in M$ and all $k \in G$, and, further, to $\vartheta(g,h)c = c$ for all $c \in M$ and $g \in G$. However, that means $h \in T_\lambda \cap T_\rho$.

The element z belongs to N_ρ exactly when $L(x,y)$ fixes z for all $x, y \in Q$. Choosing $a = 0$ yields $c \in A$, and choosing $g = 1$ yields $(\vartheta(h,k)^{-1} - 1)a = 0$. Therefore $k \in T_\rho$. The converse direction is clear.

Finally, $x \in N_\lambda$ whenever $L(x,y) = \mathrm{id}_Q$ for all $y \in Q$. We obtain $g \in T_\lambda$ by choosing $k = 1$. If $g \in T_\lambda$, then the term $\vartheta(g,h)$ can be ignored, and the condition reduces to $(\vartheta(h,k)^{-1} - 1)a = 0$, for all $h, k \in G$. □

Note that $T_\lambda = \{g \in G;\ \vartheta(g,h) = 1$ for all $h \in G\}$ if the module M is faithful. For T_ρ one can make a mirror observation. In this paper we are mainly interested in the case of commutative Q, $Z(Q) = 1$. In that case we have $T = T_\lambda = T_\rho$ and $Z(Q) = A \times T$. Therefore the assumption $N_\lambda = N_\rho = 1$ implies $Z(Q) = 1$ if Q is commutative.

The set $0 \times G$ is a subgroup of Q that complements $M \times 1 \trianglelefteq Q$. For classification purposes it is useful to know how many such complements exist and how they interact. Each of them has the form $\{(\tau(g), g);\ g \in G\}$, where $\tau : G \to M$ is a mapping, $\tau(1) = 0$. If this set is a subgroup, then $L(x,y)$ always fixes z when $x = (\tau(g), g)$, $y = (\tau(h), h)$ and $z = (\tau(k), k)$, for all $g, h, k \in G$.

By Proposition 2.1 this reduces to $(\vartheta(h,k)^{-1} - 1)\tau(g) + \tau(k) = \vartheta(g,h)^{-1}\tau(k)$. We can hence state

Lemma 2.6. *Let* $\tau : G \to M$ *be a mapping,* $\tau(1) = 0$. *The set* $\{(\tau(g), g);\ g \in G\}$ *is a subgroup of* Q *if and only if the equalities*

$$\tau(k) - \tau(g) = \vartheta(g,h)^{-1}\tau(k) - \vartheta(h,k)^{-1}\tau(g), \quad \text{and}$$
$$\tau(g) + \tau(h) = \vartheta(g,h)^{-1}\tau(gh)$$

hold for all $g, h, k \in G$.

We now turn to questions of isomorphisms. More exactly, we shall mention those few facts that can be easily stated on this general level.

Lemma 2.7. *Let* $Q = [M, G, \vartheta]$. *If* α *is an automorphism of the* R*-module* M, *then* $(a,g) \mapsto (\alpha(a), g)$ *is an automorphism of* Q.

Proof: Indeed, $(\alpha(a), g)(\alpha(b), h) = (\vartheta(g,h)(\alpha(a) + \alpha(b)), gh) = (\alpha(\vartheta(g,h)(a + b)), gh)$, for all $g, h \in G$ and $a, b \in M$. □

Lemma 2.8. *Let $Q_i = [M_i, G_i, \vartheta_i]$ for $i \in \{1,2\}$. An isomorphism $Q_1 \cong Q_2$ that maps $0 \times G_1$ upon $0 \times G_2$ and $M_1 \times 1$ upon $M_2 \times 1$ exists if and only if there exist group isomorphisms $\alpha : M_1(+) \cong M_2(+)$ and $\beta : G_1(\cdot) \cong G_2(\cdot)$ such that*

$$\alpha(\vartheta_1(g,h)a) = \vartheta_2(\beta(g),\beta(h))\alpha(a) \quad \text{for all} \quad a \in M_1 \quad \text{and} \quad g,h \in G_1.$$

Proof: This is a direct translation of the isomorphism condition. □

By coupling Lemmas 2.7 and 2.8 we obtain

Corollary 2.9. *Let $Q_i = [M_i, G_i, \vartheta_i]$ for $i \in \{1,2\}$, and suppose that M_1 and M_2 coincide as groups and that the group $\operatorname{Aut} M_1(+)$ is abelian. An isomorphism $Q_1 \cong Q_2$ that maps $0 \times G_1$ upon $0 \times G_2$ and $M_1 \times 1$ upon $M_2 \times 1$ exists if and only if there exists a group isomorphism $\beta : G_1(\cdot) \cong G_2(\cdot)$ such that $\vartheta_1(g,h)a = \vartheta_2(\beta(g),\beta(h))a$, for all $g,h \in G_1$ and $a \in M_1$.*

3. Loops from fractional mappings

Start by assuming that $Q = [M, G, \vartheta]$ is the loop of Proposition 2.1, with ϑ being commutative. Then all $L(x,y)$ generate $\operatorname{Inn} Q$, and $\operatorname{Inn} Q$ has a normal subgroup, say S, that is generated by mappings

$$(c,k) \mapsto (c + (\vartheta(h,k)^{-1} - 1)a, k).$$

It is not difficult to see that the structure of S is influenced by the behaviour of the ratio mappings $k \mapsto (\vartheta(h,k)^{-1} - 1)/(\vartheta(h',k)^{-1} - 1)$, where h, h' are constants that run through G. These mappings have to have a specific form when the structure of S should also be specific — say cyclic. This is, roughly speaking, the reason why our further investigations here are limited to what seems to be a rather special form for mappings ϑ. Detailed arguments why no other cocycles need to be considered will appear in future classification papers dealing with the situation of $|\operatorname{Inn} Q| = pq$, and with the (more general) situation of $\operatorname{Inn} Q$ metacyclic.

For $\vartheta : G \times G \to R^*$ and $h,k \in G$ set $\vartheta^{-1}(h,k) = (\vartheta(h,k))^{-1}$. Clearly $\vartheta \in \varGamma^2(G,R^*)$ if and only if $\vartheta^{-1} \in \varGamma^2(G,R^*)$. We shall be applying the construction of Proposition 2.1 to $\vartheta = \sigma^{-1}$, where σ is a 2-cocycle derived from Proposition 1.4 in the following way.

Let $f(x) = (sx+r)/(tx+1)$ be a 0-bijective linear fractional mapping $R \to R$, where R is a commutative ring. Let k be the size of the set $\{f^i(0); i \in \mathbb{Z}\}$. We shall call k the 0-*order* of f. By Proposition 1.4 the mapping $(i,j) \mapsto 1 + tr^{-1} f^i(0) f^j(0)$ is a 2-cocycle from $\varGamma^2(\mathbb{Z}, R^*)$. Regard now the mapping γ, $\gamma(i) = f^i(0)$ as a mapping $\mathbb{Z}_{k'} \to R$, where $k' \geq 0$ is a multiple of k (including the case $k' = \infty$). It is clear that

$$\sigma(i,j) = 1 + tr^{-1}\gamma(i)\gamma(j)$$

yields a 2-cocycle from $\Gamma^2(\mathbb{Z}_{k'}, R^*)$. Put $g(x) = (sx+1)/(rtx+1)$. Then

$$\sigma(i,j) = 1 + trr^{-1}f^i(0)r^{-1}f^j(0) = 1 + trg^i(0)g^j(0),$$

by Lemma 1.5. We see that the for the loop constructions we can consider only the case $r = 1$, without loss of generality.

If $k' > k$, then $\sigma(k,j) = \sigma(j,k) = 1$, for all $j \in \mathbb{Z}_{k'}$. In such a case $k \neq 0$, and hence $Z(Q) \neq 1$, by Lemma 2.5. Since we are interested chiefly in centerless loops, we shall assume $k' = k$ from here on.

Proposition 3.1. *Let M be a module over a commutative ring R, and let $f : R \to R$ be a 0-bijective fractional linear mapping of 0-order k, $f(x) = (sx + 1)/(tx+1)$. Define a loop $Q = M[s,t]$ on $M \times \mathbb{Z}_k$ by*

$$(a,i)\cdot(b,j) = \left(\frac{a+b}{1+tf^i(0)f^j(0)},\, i+j\right).$$

If $\delta \in M$ and $\lambda \in R^*$, then $\tau_\delta : (b,j) \mapsto (b + f^j(0)\delta, j)$ and $\mu_\lambda : (b,j) \mapsto (\lambda b, j)$ are permutations of Q, and $\operatorname{Inn} Q$ is the semidirect product of groups $\{\tau_\delta;\ \delta \in tM\} \trianglelefteq \operatorname{Inn} Q$ and $\{\mu_\lambda;\ \lambda \in G\}$, where $G = \langle 1 + tf^i(0)f^j(0);\ i,j \in \mathbb{Z}\rangle \le R^*$. The operation $(\delta,\lambda)(\delta',\lambda') = (\delta + \lambda\delta', \lambda\lambda')$ defines a group upon $tM \times G$, and this group can be mapped homomorphically upon $\operatorname{Inn} Q$ by $(\delta,\lambda) \mapsto \tau_\delta\mu_\lambda$. The homomorphism becomes an isomorphism when the submodule tM is faithful.

Proof: We have already observed that the loop Q is constructed by the method of Proposition 2.1, with $\vartheta(i,j)^{-1} = 1 + t\gamma(i)\gamma(j)$. The loop is commutative, and hence $\operatorname{Inn} Q$ is generated by mappings

$$(c,h) \mapsto \left(\frac{t\gamma(j)\gamma(h)a + c}{1 + t\gamma(i)\gamma(j)},\, h\right),$$

again by Proposition 2.1. This mapping can be expressed as $\mu_\lambda\tau_\delta$, where $\delta = t\gamma(j)a$ and $\lambda = (1 + t\gamma(i)\gamma(j))^{-1}$. If $i = 0$, then μ_λ is trivial, and any element of R can be in place of δ since t is invertible and $\gamma(1) = 1$. The mapping $\mu_\lambda\tau_\delta\mu_\lambda^{-1}$ clearly sends each (c,h) to $(\lambda(\delta\gamma(h) + \lambda^{-1}c), h) = \tau_{\lambda\delta}(c,h)$, and the rest is easy. □

Let $Q = M[s,t]$ be the loop of Proposition 3.1, with $k > 1$. Suppose that $j \in \mathbb{Z}_k$ satisfies $tf^i(0)f^j(0) + 1 = 1$ for all $i \in \mathbb{Z}_k$. This is equivalent to $tf^j(0) = 0$ since $f(0) = 1$. From Lemma 2.5 we immediately derive the following description of the nuclei and the center.

Proposition 3.2. *Let $Q = M[s,t]$, where M is a faithful module over a commutative ring R. Then $N_\lambda = N_\rho = Z(Q) = A \times T$ and $N_\mu = M \times T$, where $A = \{a \in M;\ ta = 0\}$ and $T = \{j \in \mathbb{Z}_k;\ tf^j(0) = 0\}$.*

Proposition 3.3. *Let $Q = M[s,t]$, where M is a faithful module over a commutative ring R. If $t \in R^*$, then $N_\lambda = N_\rho = Z(Q) = 1$, $N_\mu = M \times 1$, and $Z(\operatorname{Inn} Q) = 1$. On the other hand if tM is finite and $Z(Q) = 1$, then $t \in R^*$.*

Proof: Most of the claims follow immediately from Proposition 3.2. Suppose that tM is finite and $Z(Q) = 1$. The group endomorphism $a \mapsto ta$ of M is assumed, by Proposition 3.2, to possess a trivial kernel, and hence M has to be finite as well. If $ta = tb$ for some $a, b \in M$, then $t(a-b) = 0$, $a - b \in Z(Q)$ and $a = b$. The scalar multiplication by t thus permutes M, and there exists $m \geq 1$ such that $t^m a = a$ for all $a \in A$. That means $t^m = 1$ since M is assumed to be faithful, and thus $t \in R^*$.

Assume $t \in R^*$. It remains to prove that then $Z(\operatorname{Inn} Q) = 1$. We have $\operatorname{Inn} Q \cong H$, where H is the semidirect product $M(+) \rtimes G$, $(a,g)(b,h) = (a + gb, gh)$, by Proposition 3.1. If $gb = b$ for all $g \in G$, then $(1+t)b = b$ and $b = 0$ since $t \in G$. If $gb = b$ for all $b \in M$, then $g = 1$ since M is assumed to be faithful. □

We are mainly interested in finite loops with metacyclic inner mapping groups that have a trivial center. Therefore we shall be usually assuming $t \in R^*$.

Let us have $Q = M[s,t]$, where $t \in R^*$. We shall investigate the existence of group complements to $M \times 1$. The first equality of Lemma 2.6 can be written as $t\gamma(h)(\gamma(i)\tau(j) - \gamma(j)\tau(i)) = 0$, where $\gamma(i)$ stands, as usual, for $f^i(0)$. Since $\gamma(1) = 1$ and $t \in R^*$, this equality yields $\gamma(i)\tau(j) - \gamma(j)\tau(i) = 0$, and thus the choice $i = 1$ supplies a definition of τ by means of $d = \tau(1)$ and of γ, namely

$$\tau(j) = \gamma(j)d \quad \text{for all} \quad j \in \mathbb{Z}.$$

The second formula of Lemma 2.6 turns into the equality

$$\tau(i) + \tau(j) - \tau(i+j) = t\gamma(i)\gamma(j)\tau(i+j),$$

which we shall now investigate. Lemma 1.2 can be used to express $\tau(i+j)$ as $d(i,j)(\gamma(i) + \gamma(j) + (s-1)\gamma(i)\gamma(j))$, where $d(i,j) = d/(1 + t\gamma(i)\gamma(j))$. The left hand side is equal to

$$d(i,j)\gamma(i)\gamma(j)(t\gamma(i) + t\gamma(j) - (s-1)),$$

and the right hand side to

$$d(i,j)\gamma(i)\gamma(j)(t\gamma(i) + t\gamma(j) + t(s-1)\gamma(i)\gamma(j)).$$

The equality therefore holds for all $i, j \in \mathbb{Z}$ if and only if

$$d(s-1)\gamma(i)\gamma(j)(1 + t\gamma(i)\gamma(j)) = 0.$$

The element $1 + t\gamma(i)\gamma(j)$ is always invertible, and $\gamma(1) = 1$. The equality is hence true if and only if $d(s-1) = 0$. We can state

Proposition 3.4. *Let $Q = M[s,t]$, where M is a faithful module over a commutative ring R and $s,t \in R^*$. Then every group complement to $N_\mu = M \times \{0\}$ is determined by $d \in M$ such that $(s-1)d = 0$ and equals $\{(i, f^i(0)d);\ i \in \mathbb{Z}_k\}$, where k is the 0-order of the 0-bijective linear fractional mapping $f : x \mapsto (sx+1)/(tx+1)$.*

Proposition 3.5. *Let $Q = M[s,t]$, where M is a faithful module over a commutative ring R and $s,t \in R^*$. If H_1 and H_2 are two group complements to N_μ, then there exists $\alpha \in \operatorname{Aut} Q$ such that $\alpha(x) = x$ for all $x \in N_\mu$, $\alpha(xN_\mu) = xN_\mu$ for all $x \in Q$ and $\alpha(H_1) = H_2$.*

Proof: The group complement has the form $\{(\gamma(i)d, i);\ i \in \mathbb{Z}_k\}$, $d(s-1) = 0$, by Proposition 3.4. Let it be the group H_2. We can assume that $H_1 = 0 \times \mathbb{Z}_k$. Define $\alpha : Q \to Q$ by $(a,i) \mapsto (a + \gamma(i)d, i)$.

Choose $a,b \in M$ and $i,j \in \mathbb{Z}_k$, and set $u = (1 + t\gamma(i)\gamma(j))^{-1}$. We wish to verify that $(a+\gamma(i)d, i)(b+\gamma(j)d, j) = (u(a+b+\gamma(i)d+\gamma(j)d), i+j)$ coincides with $(u(a+b)+\gamma(i+j)d, i+j)$. By Lemma 1.2, $d\gamma(i+j) = ud(\gamma(i)+\gamma(j)+(s-1)\gamma(i)\gamma(j))$. This equals $u(d\gamma(i) + d\gamma(j))$ since $d(s-1) = 0$, by Proposition 3.4. □

Let us return once more to Proposition 3.1. The mappings μ_λ are automorphisms of Q, by Lemma 2.7. The mapping τ_δ is an automorphism if $\gamma(i+j)(1 + t\gamma(i)\gamma(j))\delta = (\gamma(i) + \gamma(j))\delta$, for all $i,j \in \mathbb{Z}_k$. This is equivalent to $(s-1)\gamma(i)\gamma(j)\delta = 0$, by Lemma 1.2, and thus to $(s-1)\delta = 0$. We can state

Theorem 3.6. *Let $Q = M[s,t]$, where M is a module over a commutative ring R. If $s = 1$, then Q is an A-loop. If $t \in R^*$, the module M is faithful and Q is an A-loop, then $s = 1$.*

4. The question of isomorphism

In the first part of this section we adopt notational conventions of Section 1. By f we shall denote a 0-bijective linear fractional mapping $R \to R$, $f(x) = (ax+b)/(cx+1)$. Recall that $a,b \in R^*$, by Lemma 1.1.

We shall assume that f is of a finite 0-order k, and that $r, \bar{r} \in \mathbb{Z}_k$ satisfy $r\bar{r} \equiv 1 \bmod k$. Our aim is to prove that there exists a 0-bijective linear fractional mapping g such that $g^i(0) = f^{ri}(0)$.

Put $d = f^r(0)$. Our candidate for g will be the partial mapping $R \to R$,

$$x \mapsto \frac{(b + da - d)x + db}{cdx + b}$$

that is considered as defined when $cdx + b \in R^*$. We shall denote this mapping by g and we shall prove that it satisfies all of the required properties.

Lemma 4.1. *The value $g^i(0)$ is defined for all $i \geq 0$, with $g^i(0) = f^{ri}(0)$ for all $i \geq 0$.*

Proof: We shall proceed by induction. The case $i = 0$ is trivial. Lemma 1.2 can be used to prove the induction step since $d = f^r(0)$:

$$\begin{aligned} g^{i+1}(0) = g(f^{ri}(0)) &= \frac{(b+da-d)f^{ri}(0)+bd}{cdf^{ri}(0)+b} \\ &= \frac{bf^r(0)+bf^{ri}(0)+(a-1)f^r(0)f^{ri}(0)}{b+cf^r(0)f^{ri}(0)} = f^{r+ri}(0) = f^{r(i+1)}(0). \end{aligned}$$

□

Lemma 4.2. *The element $g^i(0)$ belongs to dR, for every $i \geq 0$.*

Proof: Proceed by induction on $i \geq 0$. If $g^i(0) = dy$, then $g^{i+1}(0) = d((b+da-d)y+b)/u$, where $u = cdg^i(0)+b$ is invertible, by Lemma 4.1. □

The above two lemmas hold for all $r \in \mathbb{Z}_k$. If r is coprime to k, which we assume, then $b = f(0) = g^{\bar{r}}(0)$ is a multiple of d, by Lemma 4.2, and hence $d = f^r(0) = g(0) \in R^*$. To show that g is a 0-bijective linear fractional mapping, it thus remains to prove the invertibility of g, i.e. the invertibility of $b(b+da-d)-(cd)(db)$.

By Lemma 1.1, $f^{-1}(x) = (a^{-1}x - ba^{-1})/(-ca^{-1}x+1)$. By Lemma 4.1, $f^{-ri}(0) = h^r(0)$, where h is defined as

$$x \mapsto \frac{(-b+d'-d'a)x-d'b}{-cd'x-b} = \frac{(b+d'a-d')x+d'b}{cd'x+b},$$

where $d' = f^{-r}(0) \in R^*$. Furthermore, $f^0(0) = f^{r-r}(0)$, and hence $b(d+d')+(a-1)dd' = 0$, by Lemma 1.2. Thus $-bd = d'((a-1)d+b) \in R^*$, $(a-1)d+b \in R^*$ and $d' = -bd((a-1)d+b)^{-1}$. The fraction used when computing $g(d')$ gives $cdd'+b \in R^*$, and by substituting for d' we obtain $-bcd^2+b^2+b(a-1)d = b(b+da-d)-(cd)(bd) \in R^*$. Thus g is really a linear fractional mapping. We have proved

Proposition 4.3. *Let R be a commutative ring and let $f : R \to R$ be a 0-bijective linear fractional mapping of a finite 0-order k. Suppose that $r < k$ is a positive integer coprime to k, and put $d = f^r(0)$. Then $d \in R^*$ and*

$$g : x \mapsto \frac{(b+da-d)x+db}{cdx+b}$$

defines a 0-bijective linear fractional mapping such that $g^i(0) = f^{ri}(0)$ for all $i \in \mathbb{Z}$.

We shall now show how Proposition 4.3 can be used to establish isomorphisms between loops of the form $M[s,t]$.

Lemma 4.4. *Let $Q = M[s,t]$, where M is a module over a commutative ring R, and $s,t \in R^*$. Let $k < \infty$ be the 0-order of the linear fractional mapping $f : x \mapsto (sx+1)/(tx+1)$, and let r be coprime to k, $1 \le r < k$. Then $d = f^r(0) \in R^*$, and there exists a loop $M[\bar{s},\bar{t}]$ with parameters $\bar{s} = 1 + ds - d$ and $\bar{t} = td^2$. Furthermore, $(a,i) \mapsto (a,ri)$ maps this loop isomorphically upon $Q = M[s,t]$.*

Proof: From Proposition 4.3 and Lemma 1.5 we see that

$$h : x \mapsto \frac{(1+ds-d)x+1}{td^2x+1}$$

defines a 0-bijective linear fractional mapping such that $h^i(0) = d^{-1}f^{ri}(0)$ for all $i \in \mathbb{Z}$.

The product of (a,i) and (b,j) in $M[1+ds-d, td^2]$ is equal to $((a+b)/u, i+j)$, where $u = 1 + td^2h^i(0)h^j(0) = 1 + tf^{ri}(0)f^{rj}(0)$, while the product of (a,ri) and (b,rj) in $M[s,t]$ is equal to $((a+b)/u, r(i+j))$. The rest is clear. $\square$

Let us now ask when $Q = M[s,t]$ and $\bar{Q} = M[\bar{s},\bar{t}]$ are isomorphic, where M is a faithful module over a commutative ring R, and $s,t,\bar{s},\bar{t} \in R^*$. An isomorphism has to map $N_\mu(Q)$ upon $N_\mu(\bar{Q})$, and therefore we may assume that $M \times 0$ is mapped upon itself, by Proposition 3.3. We shall assume that the 0-order k is finite. An isomorphism may be composed with an automorphism of Proposition 3.5, and therefore we may assume that $0 \times \mathbb{Z}_k$ is mapped upon itself as well. This mapping has to have the form $i \mapsto \bar{r}i$, where $\bar{r}r \equiv 1 \bmod k$ for some $r, \bar{r} \in \mathbb{Z}_k$. Let us have $f(x) = (sx+1)/(tx+1)$ and $h(x) = (\bar{s}x+1)/(\bar{t}x+1)$, where $s,t,\bar{s},\bar{t} \in R^*$. The condition of Lemma 2.8 takes the form

$$\alpha\left(\frac{a}{1+tf^{ri}(0)f^{rj}(0)}\right) = \frac{\alpha(a)}{1+\bar{t}h^i(0)h^j(0)}\,.$$

If α is an isomorphism of modules, then this can be further reduced to

$$tf^{ri}(0)f^{rj}(0) = \bar{t}h^i(0)h^j(0) \ \text{ for all } \ i,j \in \mathbb{Z}$$

since M is assumed to be faithful. Such a reduction can be always done when $M(+)$ is a cyclic group, by Corollary 2.9. Let us hence assume that the equality holds.

The choice $i = j = 1$ yields $td^2 = \bar{t}$, where $d = f^r(0)$, and the choice $j = 1$ gives $h^i(0) = d^{-1}f^{ri}(0)$. Such a definition of h fulfils the equality above, and we see from Lemma 4.4 that $\bar{s} = 1 + ds - d$ when α is the identity mapping. (The values $\bar{s}$ and $\bar{t}$ can be deduced from the operation of $M[\bar{s},\bar{t}]$, and hence they are uniquely defined.) Using Lemma 2.7 we can thus state

Proposition 4.5. *Let M be a faithful module over a commutative ring R. Let $s, t, \bar{s}, \bar{t} \in R^*$ be such that both mappings $x \mapsto (sx+1)/(tx+1)$ and $x \mapsto (\bar{s}x+1)/(\bar{t}x+1)$ are 0-bijective of the same finite 0-order k. An isomorphism $M[s,t] \cong M[\bar{s},\bar{t}]$ which restricts to the identity upon $N_\mu = M \times 0$ exists if and only if $\bar{t} = td^2$ and $\bar{s} = 1 + ds - d$ for some $d = f^r(0)$, where $1 \le r < k$, $r \in \mathbb{Z}_k^*$. If $M(+)$ is a cyclic group, then this is a sufficient and necessary condition for the existence of any isomorphism $M[s,t] \cong M[\bar{s},\bar{t}]$.*

Let us briefly discuss whether $M[s,t]$ and $\bar{M}[\bar{s},\bar{t}]$ can be isomorphic when M is a ring over R and $\bar{M}$ is a ring over $\bar{R}$. Suppose that the corresponding loops are finite and with trivial centre. Then $M(+)$ and $\bar{M}(+)$ have to be isomorphic as groups since they yield the middle nucleus, by Proposition 3.3. We can hence assume that $M(+) = \bar{M}(+)$. The complement $0 \times \mathbb{Z}_k$ can be regarded to be the same as well, by Proposition 3.5. Furthermore, one of the loops can be replaced by an isomorphic copy (with possibly different parameters) in such a way that the isomorphism is identical on $0 \times \mathbb{Z}_k$, by Lemma 4.4. Another observation follows from the fact that both R and $\bar{R}$ can be regarded as generated by elements $a = (1 + tf^i(0)f^j(0))^{-1}$ and $\bar{a} = (1 + \bar{t}\bar{f}^i(0)\bar{f}^j(0))^{-1}$. By Lemma 2.8 there exists $\alpha \in \operatorname{Aut} M(+)$ such that $\alpha(a\alpha^{-1}(c)) = \bar{a}c$ for all $c \in M$. Since M and $\bar{M}$ are assumed to be faithful modules, we see that $R \cong \bar{R}$. We can hence consider only the situation when $R = \bar{R}$, and M and $\bar{M}$ are two R-modules, with the same underlying set and the same addition.

In such a situation one can replace $\alpha \in \operatorname{Aut} M(+)$ by the identity mapping if α is a module homomorphism, by Lemma 2.7. This always applies, as we have already remarked, to the case when $M(+) \cong \mathbb{Z}_m(+)$, which is the principal object of our interest in this paper. The general case has been reduced to possible loop isomorphisms $(a,i) \mapsto (\alpha(a), i)$, where $\alpha \in \operatorname{Aut} M(+)$, but $\alpha \notin \operatorname{Hom}_R(M, \bar{M})$. Further investigations go beyond the scope of this paper.

5. Questions of isotopism

Let Q be a loop. For each $a \in Q$ denote by $L(Q,a)$ the loop on Q with operation $a\backslash(ax \cdot y)$. Similarly, $R(Q,a)$ denotes the loop with operation $(x \cdot ya)/a$. These operations were introduced by Bruck and Paige [3], and studied extensively by Belousov [1], [2] who called them *derived* and developed a compact notational system that covers both them and the isotopes (we do not use it here). Note that L_a maps $L(Q,a)$ isomorphically upon the principal isotope $x \cdot (a\backslash y)$ of Q, and R_a connects $R(Q,a)$ with the operation $(x/a) \cdot y$. Some further standard facts are formulated in the following lemma, which is stated without a proof.

Lemma 5.1. *Let Q be a loop, and let a and b be elements of Q. Then:*

(i) *$L(L(Q,a),b) = L(Q,ab)$ and $R(R(Q,b),a) = R(Q,ab)$; and*

(ii) *L_bR_a maps isomorphically $L(R(Q,a),b)$ upon the principal isotope of Q with operation $(x/a)\cdot(b\backslash y)$, and R_aL_b is an isomorphism of $R(L(Q,b),a)$*

upon the same principal isotope.

We shall also need some easy properties that involve the middle nucleus:

Lemma 5.2. *Let Q be a loop and let a be an element of Q. Then the middle nucleus of both $L(Q,a)$ and $R(Q,a)$ coincides with that of Q. Furthermore, if $a \in N_\mu$, then $L(Q,a)$ (or $R(Q,a)$) is commutative if and only if Q is commutative. In such a case $L(Q,a) = R(Q,a)$.*

Proof: Denote by $\circ$ the operation of $L(Q,a)$. Then $x \circ (y \circ z) = a\backslash((ax) \cdot (a\backslash(ay \cdot z)))$ and $(x \circ y) \circ z = a\backslash((ax \cdot y) \cdot z)$. If $y \in N_\mu$, then $a\backslash(ay \cdot z) = yz$, and the equality $x \circ (y \circ z) = (x \circ y) \circ z$ clearly holds. If the equality holds, then $a\backslash(ay \cdot z) = yz$ follows from the choice $x = a\backslash 1$, and thus $y \in N_\mu$.

Suppose now that $a \in N_\mu$. The operation of $L(Q,a)$ is commutative if and only if the operation $(x,y) \mapsto xay$ is commutative. If that is true, then by setting $y = a^{-1}x$ we obtain $x^2 = (a^{-1}x)ax$, which gives $x = (a^{-1}x)a$ and $xa^{-1} = a^{-1}x$, for all $x \in Q$. Hence $xy = (xa^{-1})ay = ya(xa^{-1}) = y(a \cdot a^{-1}x) = yx$, for all $x, y \in Q$. If Q is commutative, then $xay = xa \cdot y = y \cdot xa = y \cdot ax = yax$. $\square$

Lemma 5.3. *Let Q be a loop in which N_μ is a normal subloop.*

(i) *If $x, y \in Q$ and $a \in N_\mu$, then there exists $b \in N_\mu$ such that*

$$L(R(L(Q,x),y),a) \cong L(L(R(Q,y),x),b).$$

(ii) *If $Q = N_\mu C$, where C is a subloop, then every loop isotope of Q is isomorphic to some*

$$L(R(L(R(Q,u),v),a),b) \quad \text{where} \quad u, v \in C \quad \text{and} \quad a, b \in N_\mu.$$

(iii) *Let $Q = N_\mu C$, where C is a subloop. If $u, v \in C$ and $a \in N_\mu$, then the loop isotope $L(L(R(Q,u),v),a)$ is commutative if and only if $L(R(Q,u),v)$ is commutative. Furthermore, each commutative loop isotope of Q can be expressed in the former form.*

Proof: To prove point (i) first note that $\varphi = [R_y, L_x]$ is an isomorphism of $R(L(Q,x),y)$ and $L(R(Q,y),x)$, by Lemma 5.1. The mapping φ also serves as an isomorphism for the corresponding derived operations, where $b = \varphi(a)$ corresponds to a. Now, N_μ is an invariant of derived operations, by Lemma 5.2, and $b = \varphi(a)$ belongs to N_μ since $N_\mu \trianglelefteq Q$ and $\varphi \in \operatorname{Inn} Q$.

To prove point (ii) consider $u, v \in C$ and $a, b \in N_\mu$, and note that $v * b = vb$, where $*$ means the operation of $R(Q,au)$. Thus $L(R(Q,au),vb)$ is isomorphic to $L(L(R(R(Q,u),a,),v),b)$, by Lemma 5.1. The exchange of the middle terms can be done by using point (i).

The commutativity does not depend upon appending an element of the middle nucleus, by Lemma 5.2. If $\bar{Q} = L(R(Q,u),v)$ is a commutative loop, then

Lemma 5.1 yields $L(R(\bar{Q},a),b) = L(L(\bar{Q},a),b) = L(\bar{Q},ab)$ since $\bar{Q}$ and Q coincide upon N_μ. Point (iii) thus follows from point (ii). □

Let us turn again to the loops $Q = M[s,t]$ as introduced in Proposition 3.1. We thus have $\gamma(i) = f^i(0)$, where $f(x) = (sx+1)/(tx+1)$, and $(a,i)(b,j) = ((1+t\gamma(i)\gamma(j))^{-1}(a+b), i+j)$. Our intention is to study the cases where each commutative isotope of Q is isomorphic to some $M[\bar{s},\bar{t}]$.

From Lemma 5.3 we see that we can concentrate upon the loops $L(Q,(c,0))$ and $L(R(Q,(0,g)),(0,h))$.

Denote first by $\circ$ the operation of $L(Q,(c,0))$. This operation is always commutative, by Lemma 5.2 and Proposition 3.2. In fact, it is easy to give an exact formula, and we obtain

$$(a,i)\circ(b,j) = \left(\frac{a+b-t\gamma(i)\gamma(j)c}{1+t\gamma(i)\gamma(j)},\, i+j\right).$$

To find in $Q(\circ)$ a group complement to $M\times 0$ we shall proceed as in Lemma 2.2, i.e. we shall try to identify those $x = (a,i)$ for which the triple (x,x,x^{-1}) is associative. We see that the inverse to (a,i) in $Q(\circ)$ is equal to $(t\gamma(i)\gamma(-i)c - a, -i)$, and that

$$(a,i)\circ(a,i) = \left(\frac{2a-ty^2c}{1+ty^2}, 2i\right), \quad \text{where } \; y = \gamma(i).$$

There exists $b \in M$ such that

$$((a,i)\circ(a,i))\circ(t\gamma(i)\gamma(-i)c - a, -i) = (b,i).$$

Our intention is to evaluate b and to give conditions under which $a = b$. Set $s' = s-1$ and $y = \gamma(i)$. We shall need

Lemma 5.4. *The element $1+s'\gamma(i)$ is invertible for every $i \in \mathbb{Z}$.*

Proof: By Lemma 1.2, $0 = \gamma(-i)+\gamma(i)+s'\gamma(i)\gamma(-i)$. Therefore $(1+s'\gamma(i))(1+s'\gamma(-i)) = 1+s'(\gamma(i)+\gamma(-i)+s'\gamma(i)\gamma(-i)) = 1$. □

From Lemma 1.2 and Lemma 5.4 we easily obtain

$$\gamma(-i) = \frac{-y}{1+s'y} \quad \text{and} \quad \gamma(2i) = \frac{2y+s'y^2}{1+ty^2}. \;\text{ Thus}$$

$$b = (1+t\gamma(-i)\gamma(2i))^{-1}\left(\frac{-ty^2}{1+s'y}c - a + \frac{2a-ty^2c}{1+ty^2} - t\gamma(-i)\gamma(2i)c\right),$$

$$\gamma(-i)\gamma(2i) = -y^2(s'y+2)(1+s'y)^{-1}(1+ty^2)^{-1} \quad \text{and}$$

$$(1+t\gamma(-i)\gamma(2i))^{-1} = (1+s'y)(1+ty^2)e^{-1},$$

$$\text{where } \; e = (1+s'y)(1+ty^2) - ty^2(s'y+2) = 1+s'y-ty^2.$$

Hence $b = e^{-1}b'$, where $b' = (1+ty^2)(-ty^2)c - (1+s'y)(1+ty^2)a + (1+s'y)(2a - ty^2c) + ty^2(s'y+2)c = (1+s'y)(1-ty^2)a - t^2y^4c$. The equality $a = b$ thus leads to

$$(1+s'y)(1-ty^2)a - t^2y^4c = (1+s'y-ty^2)a.$$

After subtracting $(1+s'y)a - ty^2a$ from both sides we cancel t (c.f. Proposition 3.3). We get $s'y^3a + ty^4c = 0$. Now, $y = f^i(0)$ has to be invertible in many cases, c.f. Lemma 4.4. If it is invertible, then $s'a = -tf^i(0)c$ and $c \in s'M$. This is a necessary condition for the existence of a group complement to N_μ in $Q(\circ)$ if $t \in R^*$. By the next statement, $Q(\circ) \cong Q(\cdot)$ if $c \in s'M$, and so this condition is also sufficient.

Proposition 5.5. *Assume $Q = M[s,t]$, where M is a module over a commutative ring R. Denote by f the linear fractional mapping $x \mapsto (sx+1)/(tx+1)$, and assume that $c = (s-1)d$ for come $c, d \in M$. Then $(a,i) \mapsto (-tf^i(0)d + a, i)$ yields an isomorphism $Q \cong L(Q,(c,0))$. On the other hand, if $c \notin (s-1)M$, and $t \in R^*$, then the middle nucleus of $L(Q,(c,0))$ possesses no group complement.*

Proof: We need only to prove that the described mapping is an isomorphism. Note that $-t\gamma(i+j)d$ is equal to the product of $-t(\gamma(i)+\gamma(j))d - t\gamma(i)\gamma(j)$ with $(1+t\gamma(i)\gamma(j))^{-1}$, by Lemma 1.2. Hence the product of $(-t\gamma(i)d + a, i)$ and $(-t\gamma(j)d + b, j)$ in $L(Q,(c,0))$ is equal to

$$\left(\frac{-t(\gamma(i)+\gamma(j))d - t\gamma(i)\gamma(j)c + a + b}{1+t\gamma(i)\gamma(j)}, i+j\right) = \left(-t\gamma(i+j)d + \frac{a+b}{1+t\gamma(i)\gamma(j)}, i+j\right). \qquad \square$$

6. Isotopes and fractional mappings

Our aim is to describe all commutative isotopes of $Q = M[s,t]$ that possess a group complement to N_μ. By Lemma 5.3 we need now to find the commutative isotopes of the form $L(R(Q,(0,g)),(0,h))$.

Proposition 6.1. *Assume $Q = M[s,t]$, where M is a faithful module over a commutative ring R, and $s, t \in R^*$. Denote by k the 0-order of the 0-bijective fractional linear mapping $f : x \mapsto (sx+1)/(tx+1)$. The principal isotope of Q with operation*

$$(a,i) \circ (b,j) = ((a,i)/(0,g)) \cdot ((0,h)\backslash(b,j))$$

is commutative if and only if $g = h$, for all $g, h \in \mathbb{Z}_k$.

Proof: We have $(a,i)/(0,g) = (0,g)\backslash(a,i) = ((1+t\gamma(i-g)\gamma(g))a, i-g)$, and therefore $(a,i) \circ (b,j)$ is the product (in Q) of $((1+t\gamma(i-g)\gamma(g))a, i-g)$ and

$((1+t\gamma(j-h)\gamma(h))b, j-h)$, while $(b,j)\circ(a,i)$ equals the product of $((1+t\gamma(i-h)\gamma(h))a, i-h)$ and $((1+t\gamma(j-g)\gamma(g))b, j-g)$. By analyzing the case $b=0$ we see that the commutativity of $\circ$ implies

$$\frac{1+t\gamma(i-g)\gamma(g)}{1+t\gamma(i-g)\gamma(j-h)} = \frac{1+t\gamma(i-h)\gamma(h)}{1+t\gamma(i-h)\gamma(j-g)}\,.$$

If $i=g$, then $\gamma(g-h)\gamma(h)=\gamma(g-h)\gamma(j-g)$, and by setting $j=g$ we obtain $\gamma(g-h)\gamma(h)=0$. Thus $\gamma(g-h)\gamma(j-g)=0$ for all $j\in\mathbb{Z}$, and the choice $j=g+1$ brings $\gamma(g-h)=0$. Therefore the commutativity of $Q(\circ)$ implies $g=h$. □

To be able to analyze the loops of Proposition 6.1, we need several auxiliary statements that involve 0-bijective fractional linear mappings. Let $f:(sx+1)/(tx+1)$ be such a mapping, and let k be the 0-order of f. As elsewhere, we often write $\gamma(i)$ in place of $f^i(0)$ and s' in place of $s-1$.

Lemma 6.2. *The element $1+s'\gamma(i)-t\gamma(i)\gamma(j)$ is invertible for all $i,j\in\mathbb{Z}$.*

Proof: We have $\gamma(-i)=-\gamma(i)/(1+s'\gamma(i))$, by Lemmas 1.2 and 5.4. The element $1+t\gamma(-i)\gamma(j)$ is invertible, by Lemma 1.2. Our result thus follows immediately after making the substitution for $\gamma(-i)$. □

Lemma 6.3. *Fix $g\in\mathbb{Z}$. Then the mapping*

$$\varphi : x\mapsto \frac{(s-t\gamma(g))x+s'\gamma(g)+1-t\gamma(g)^2}{tx+t\gamma(g)+1}$$

is a 0-bijective linear fractional mapping that satisfies $\varphi^i(0)=\gamma(i+g)-\gamma(g)$ for every $i\in\mathbb{Z}$.

Proof: First note that $(s-t\gamma(g))(t\gamma(g)+1)-t(s'\gamma(g)+1-t\gamma(g)^2)=s-t\in R^*$. Thus φ fulfils our definition of a fractional linear mapping, and as such it is injective. The element $\varphi(0)$ is invertible, by Lemmas 6.2 and 1.2. To finish the proof it therefore suffices to show the formula for $\varphi^i(0)$. We shall assume $i\geq 0$, which suffices for the case of finite 0-order k. (The proof for $i<0$ can be obtained either directly, or by considering the mapping f^{-1}.)

We have $\varphi(0)=(1+s'\gamma(g)-t\gamma(g)^2)/(1+t\gamma(g))=\gamma(g+1)-\gamma(g)$. By using induction, we obtain

$$\begin{aligned}\gamma(i+g+1)-\gamma(g) &= \frac{s\gamma(i+g)+1}{t\gamma(i+g)+1}-\gamma(g)\\ &= \frac{(s-t\gamma(g))(\gamma(i+g)-\gamma(g))+s'\gamma(g)+1-t\gamma(g)^2}{t(\gamma(i+g)-\gamma(g))+t\gamma(g)+1}\\ &= \varphi(\gamma(i+g)-\gamma(g))=\varphi(\varphi^i(0))=\varphi^{i+1}(0).\end{aligned}$$

□

Corollary 6.4. *Fix $g \in \mathbb{Z}$ and put $s_g = (s - t\gamma(g))/(t\gamma(g)+1)$ and $t_g = t(1 + s'\gamma(g) - t\gamma(g)^2)/(t\gamma(g)+1)^2$, where $s' = s - 1$. Then the mapping $f_g : x \mapsto (s_g x + 1)/(t_g x + 1)$ is a* 0*-bijective linear fractional mapping such that*

$$\gamma_g(i) = f_g^i(0) = \frac{1 + t\gamma(g)}{1 + s'\gamma(g) - t\gamma(g)^2}(\gamma(i+g) - \gamma(g)), \quad \textit{for all} \;\; i \in \mathbb{Z}.$$

Proof: This follows directly from Lemmas 6.3 and 1.5. □

From Proposition 6.1 we know that to understand the commutative isotopes of $M[s,t]$, it remains to investigate the operation $((a,i)/(0,g)) \cdot ((0,g)\backslash(b,j))$, where $g \in \mathbb{Z}_k$. There exist various isomorphic copies of this operation, and the next lemma describes the one that we shall use in further calculations.

Lemma 6.5. *Fix $g \in \mathbb{Z}$ and define operation $*_g$ upon Q by*

$$(a,i) *_g (b,j) = \left(\frac{a + b + t\gamma(g)(\gamma(i)a + \gamma(j)b)}{1 + t\gamma(i)\gamma(j)}, \, i + j - g \right).$$

Then $Q(*_g)$ is a loop and $(a,i) \mapsto (a, i+g)$ gives an isomorphism between this loop and the isotope of Q with operation $((a,i)/(0,g)) \cdot ((0,g)\backslash(b,j))$.

Proof: Recall that $(a,i)/(0,g) = (0,g)\backslash(a,i) = ((1 + t\gamma(i-g)\gamma(g))a, i - g)$, for all $(a,i) \in Q$. The product of $(a, i+g)$ and $(b, j+g)$ in the isotope is thus equal to $(c, i+j)$, where $(1 + t\gamma(i)\gamma(j))c = a + b + t\gamma(g)(\gamma(i)a + \gamma(j)b)$. We also obtain $(a,i) *_g (b,j) = (c, i+j-g)$, and the rest is clear. □

We shall now perform the crucial calculations of this section.

Lemma 6.6. *The mapping $(a,i) \mapsto ((1 + t\gamma(i+g)\gamma(g))^{-1}a, \, i+g)$ yields an isomorphism $M[s_g, t_g] \cong Q(*_g)$, for any $g \in \mathbb{Z}$.*

Proof: We need to prove the equality

$$\begin{aligned} ((1 + t\gamma(i+j+g)\gamma(g))^{-1}&(1 + t_g\gamma_g(i)\gamma_g(j))^{-1}(a+b), \, i+j+g) \\ &= ((1 + t\gamma(i+g)\gamma(j+g))^{-1}(a+b), \, i+j+g), \end{aligned}$$

which we will obtain as a consequence of

$$1 + t\gamma(i+g)\gamma(j+g) = (1 + t\gamma(i+j+g)\gamma(g))(1 + t_g\gamma_g(i)\gamma_g(j)).$$

Substitutions $i \mapsto i - g$ and $j \mapsto j - g$ transform the latter equality to

$$1 + t\gamma(i)\gamma(j) = (1 + t\gamma(i+j-g)\gamma(g))(1 + t_g\gamma_g(i-g)\gamma_g(j-g)),$$

and that is the equality we shall be proving. We first need to express the term constructed from f_g. From Corollary 6.4 we easily derive that

$$t_g\gamma_g(i-g)\gamma_g(j-g) = \frac{t(\gamma(i)-\gamma(g))(\gamma(j)-\gamma(g))}{1+s'\gamma(g)-t\gamma(g)^2}\,.$$

It thus suffices to show that

$$\begin{aligned}&(1+t\gamma(i)\gamma(j))(1+s'\gamma(g)-t\gamma(g)^2)\\ &\qquad = (1+t\gamma(i+j-g)\gamma(g))(1+s'\gamma(g)+t(\gamma(i)\gamma(j)-\gamma(g)(\gamma(i)+\gamma(j)))).\end{aligned}$$

After multiplying, subtracting, and then removing $t\gamma(g)$ from all remaining summands, we see that the latter equality holds when

$$\begin{aligned}&-\gamma(g)+s'\gamma(i)\gamma(j)-t\gamma(g)\gamma(i)\gamma(j)\\ &\quad = -\gamma(i)-\gamma(j)+\gamma(i+j-g)(1+s'\gamma(g)+t(\gamma(i)\gamma(j)-\gamma(g)(\gamma(i)+\gamma(j)))).\end{aligned}$$

Since $\gamma(i)\gamma(j)(s'-t\gamma(g))-\gamma(g)+\gamma(i)+\gamma(j)$ can be expressed, by Lemma 1.2, as $\gamma(i+j)(1+t\gamma(i)\gamma(j))-t\gamma(i)\gamma(j)\gamma(g)-\gamma(g) = (\gamma(i+j)-\gamma(g))(1+t\gamma(i)\gamma(j))$, we are asking, in fact, if the latter term equals

$$\gamma(i+j-g)(1+t\gamma(i)\gamma(j)+s'\gamma(g)-t\gamma(g)(\gamma(i)+\gamma(j))).$$

For a moment denote $i+j$ by $h=(h-g)+g$. From Lemma 1.2 we obtain $\gamma(h)(1+t\gamma(h-g)\gamma(g)) = \gamma(h-g)+\gamma(g)+s'\gamma(h-g)\gamma(g)$, and thus

$$\gamma(i+j-g) = \frac{\gamma(i+j)-\gamma(g)}{1+s'\gamma(g)-t\gamma(i+j)\gamma(g)}\,,$$

by Lemma 6.2. Our equality can be thus presented as

$$\begin{aligned}&(\gamma(i+j)-\gamma(g))(1+t\gamma(i)\gamma(j))(1+s'\gamma(g)-t\gamma(i+j)\gamma(g))\\ &\qquad = (\gamma(i+j)-\gamma(g))(1+t\gamma(i)\gamma(j)+s'\gamma(g)-t\gamma(g)(\gamma(i)+\gamma(j))).\end{aligned}$$

That clearly holds if

$$-t\gamma(i+j)\gamma(g)+t\gamma(i)\gamma(j)(s'\gamma(g)-t\gamma(i+j)\gamma(g)) = -t\gamma(g)(\gamma(i)+\gamma(j)).$$

This equality will be true if

$$\gamma(i+j)(1+t\gamma(i)\gamma(j)) = s'\gamma(i)\gamma(j)+\gamma(i)+\gamma(j).$$

However, that is exactly the statement of Lemma 1.2. □

By putting together Lemma 5.3, Proposition 5.5, Corollary 6.4, Lemma 6.5 and Lemma 6.6 we obtain

Theorem 6.7. *Let $Q = M[s,t]$, where M is a faithful module over a commutative ring R, and $s,t \in R^*$. Let f be the linear fractional mapping $x \mapsto (sx+1)/(tx+1)$. For each $i \in \mathbb{Z}$ put*

$$s_i = \frac{s - tf^i(0)}{1 + tf^i(0)} \quad \text{and} \quad t_i = t\frac{1 + (s-1)f^i(0) - t(f^i(0))^2}{(1 + tf^i(0))^2}\,.$$

Then $M[s_i,t_i]$ is a commutative loop isotope of Q, and $s_i, t_i \in R^*$. Every commutative loop isotope of Q in which the middle nucleus possesses a group complement is isomorphic to such a loop. If $s_i - 1 \in R^*$ for all $i \in \mathbb{Z}$, then there exist, up to isomorphism, no other commutative loop isotopes.

Let us remark that in this section we have preferred to work with the operation $(a,i)/(0,g) \cdot (0,g)\backslash(b,j)$ rather then with $L(R(Q,(0,g)),(0,g))$. Reasons are computational. However, the operation of the latter loop is not completely inaccessible. For any commutative loop Q and any $u \in Q$, one can express the operation of $R(L(Q,u),u)$ as $L_u^{-2}(ux \cdot uy)$. We have

$$(1 + t\gamma(g)\gamma(h+g))(1 + t\gamma(g)\gamma(h)) = 1 + t\gamma(g)(2\gamma(h) + \gamma(g) + s'\gamma(h)\gamma(g)),$$

for all $g,h \in \mathbb{Z}$, by Lemma 1.2. This can be used to establish that the product of (a,i) and (b,j) in $L(R(Q,(0,g)),(0,g))$ is $(c, i+j)$, where c is equal to

$$\frac{1 + t\gamma(g)(2\gamma(i+j) + \gamma(g) + s'\gamma(i+j)\gamma(g))}{1 + t\gamma(i+g)\gamma(j+g)} \left(\frac{a}{1 + t\gamma(i)\gamma(g)} + \frac{b}{1 + t\gamma(j)\gamma(g)}\right).$$

Further simplifications are possible, again by means of Lemma 1.2. One finally obtains that the product of (a,i) and (b,j) in $L(R(Q,(0,g)),(0,g))$ is equal to

$$\left(\frac{a + b + tf^g(0)(f^j(0)a + f^i(0)b)}{1 + tf^i(0)f^j(0)},\, i+j\right).$$

7. Cyclic groups and loops

In this section we shall abandon the more general approach of the preceding sections, and will concentrate upon the case when $\operatorname{Inn} Q$ is a centerless metacyclic group, $Q = M[s,t]$, $Z(Q) = 1$. Set $m = |M|$ and let $k > 1$ be the 0-order of the 0-bijective linear fractional mapping $f : x \mapsto (sx+1)/(tx+1)$.

Suppose first that $\operatorname{Inn} Q$ is infinite. Then $\operatorname{Inn} Q$ has to be an infinite dihedral group, and $tM(+) \cong \mathbb{Z}(+)$, by Proposition 3.1. The kernel of the homomorphism $a \mapsto ta$ has to be trivial, by Proposition 3.2, and hence $M(+)$ has to be isomorphic to $\mathbb{Z}(+)$ as well. We can assume that the ring R is faithful, and thus, by standard reasoning, we can assume that $M = R = \mathbb{Z}$. Let it be the case. There are then not very many choices for s and t. Since $t+1$ should be invertible and since

$t \neq 0$, we get $t = -2$, and so $k = 2$. Therefore $s = -1$, and we get the operation $(a,i)(b,j) = ((-1)^{ij}(a+b), i+j)$ with which we started this paper. The infinite case thus brings nothing new and we can turn our attention to the finite case.

The group $\operatorname{Inn} Q$ can be expressed as the semidirect product $\mathbb{Z}_m(+) \rtimes G(\cdot)$ that naturally embeds into the holomorph of $\mathbb{Z}_m(+)$, by Propositions 3.1 and 3.3. We assume that $M = \mathbb{Z}_m(+)$ is a faithful R-module and that $G \leq R^*$ is generated by all $1 + tf^i(0)f^j(0)$. If m is even, then $\mathbb{Z}_m(+) \cong (\operatorname{Inn} Q)'$ contains exactly one involution, and this involution belongs to the center of $\operatorname{Inn} Q$. We assume $Z(\operatorname{Inn} Q) = 1$, and therefore m has to be odd. We also see that R has to be isomorphic to $\mathbb{Z}_m$ as a ring, and so we may assume $R = \mathbb{Z}_m$. We may thus investigate only loops $Q = \mathbb{Z}_m[s,t]$, where f is considered to be a linear fractional mapping $\mathbb{Z}_m \to \mathbb{Z}_m$.

Theorem 7.1. *For $m > 1$ consider $s, t, k \in \mathbb{Z}_m$ such that $f : x \mapsto (sx+1)/(tx+1)$ is a 0-bijective fractional linear mapping $\mathbb{Z}_m \to \mathbb{Z}_m$ of 0-order k. Suppose that $(a,i)(b,j) = ((a+b)/(1+tf^i(0)f^j(0)), i+j)$ defines a loop $Q = \mathbb{Z}_m[s,t]$ upon $\mathbb{Z}_m \times \mathbb{Z}_k$ with $Z(Q) = 1$ and $Z(\operatorname{Inn} Q) = 1$. Then m is odd, $s, t \in \mathbb{Z}_m^*$, $\operatorname{Inn} Q$ embeds into the holomorph of $\mathbb{Z}_m(+)$, and $\operatorname{Inn} Q \cong \mathbb{Z}_m(+) \rtimes G(\cdot)$, where $G \leq \mathbb{Z}_m^*$ is generated by all $1 + tf^i(0)f^j(0)$. The middle nucleus of Q is equal to $\mathbb{Z}_m \times 0$, and $Q[s,t] \cong Q[s',t']$ if and only if there exists $r \in \mathbb{Z}_m^*$ such that $s' = 1 + ds - d$ and $t' = td^2$, where $d = f^r(0)$.*

Proof: The statement sums up the earlier results, in particular Lemma 1.1 and Propositions 3.1, 3.3 and 4.5. □

Recall that Theorem 6.7 describes all commutative isotopes of loops $\mathbb{Z}_m[s,t]$ that possess a group complement to the middle nucleus.

Up to now we did not exhibit any examples except those with $k = 2$. Given an integer m there seems to be no immediate way how to enumerate all s and t for which $x \mapsto (sx+1)/(tx+1)$ yields a 0-bijective fractional linear mapping. However, one can build an unlimited number of examples by using a 'sieving technique': Consider first a mapping $x \mapsto (sx+1)/(tx+1)$ as a function on rational numbers. Starting from 0 we get a sequence of integer fractions a_i/b_i. Choose an odd a_k such that $b_1, \dots, b_k$ are coprime to a_k and such that $s - t$ is coprime to a_k as well. By setting $m = a_k$ and interpreting a_i/b_i in $\mathbb{Z}_m$ we get a 0-bijective fractional linear mapping $\mathbb{Z}_m \to \mathbb{Z}_m$ of 0-order k.

To get concrete examples, consider first the sequence induced by $(s,t) = (1,2)$. The sequence a_i/b_i, $0 \leq i \leq 7$, is equal to

$$\frac{0}{1}, \frac{1}{1}, \frac{2}{3}, \frac{5}{7}, \frac{12}{17}, \frac{29}{41}, \frac{70}{99} \text{ and } \frac{169}{239}.$$

The choices $k = 3, 5, 7$ fulfil our conditions and we obtain A-loops of orders $5 \cdot 3 = 15$, $29 \cdot 5 = 145$ and $169 \cdot 7 = 1183$, respectively.

For $(s,t)=(2,3)$, $0 \le i \le 7$ we get

$$\frac{0}{1},\ \frac{1}{1},\ \frac{3}{4},\ \frac{10}{13},\ \frac{33}{43},\ \frac{109}{142},\ \frac{360}{469}\ \text{and}\ \frac{1189}{1549}.$$

The choices $k \in \{2,4,5,7\}$ obviously yield loops of form $\mathbb{Z}_m[s,t]$. However, one can also use the case $k=3$ since instead of a_k one can consider any of its proper odd divisors. For $k=3$ the only choice is $m=5$ and that yields a loop of order 15. Note also that for $k \in \{2,4\}$ we do not have $t \in \mathbb{Z}_m^*$. For $k=4$ this can be rectified by setting $m=11$.

Let us finally remark that our treatment of fractional linear mappings did not rely upon matrix computation. If

$$\begin{pmatrix} s & 1 \\ t & 1 \end{pmatrix}^i \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix},$$

then $f^i(0) = a/b$, where $f : x \mapsto (sx+1)/(tx+1)$. An efficient computation of the matrix powers, either by eigenvalues or recursive polynomial formulas, could simplify some of our proofs and provide explicit formulas for the loop operation.

References

[1] Belousov V.D., *Proizvodnyje operacii i asociatory v lupach*, Mat. Sb. **45** (1958), 51–70.

[2] Belousov V.D., *Osnovy teorii kvazigrupp i lup*, Nauka, Moskva, 1967.

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

[4] Csörgő P., Niemenmaa M., *Solvability conditions for loops and groups*, J. Algebra **232** (2000), 336–342.

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

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

[7] Drápal A., *Structural interactions of conjugacy closed loops*, Trans. Amer. Math. Soc. **360** (2008), 671–689.

[8] Drápal A., Jedlička P., *On loop identities that can be obtained by a nuclear identification*, submitted.

[9] Drápal A., *A nuclear construction of loops with small inner mapping groups*, Abh. Math. Sem. Univ. Hamburg **77** (2007), 201–218.

[10] Kinyon M.K., Kunen K., Phillips J.D., *Every diassociative A-loop is Moufang*, Proc. Amer. Math. Soc. **130** (2002), 619–624.

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

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

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

Charles University, Faculty of Mathematics and Physics, Department of Algebra, Sokolovská 83, 186 75 Prague 8, Czech Republic

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

(*Received* October 5, 2007, *revised* February 7, 2008)