CONSTRUCTIONS OF COMMUTATIVE AUTOMORPHIC LOOPS

PŘEMYSL JEDLIČKA, MICHAEL K. KINYON, AND PETR VOJTĚCHOVSKÝ

Abstract. A loop whose inner mappings are automorphisms is an *automorphic loop* (or *A-loop*). We characterize commutative (A-)loops with middle nucleus of index 2 and solve the isomorphism problem. Using this characterization and certain central extensions based on trilinear forms, we construct several classes of commutative A-loops of order a power of 2. We initiate the classification of commutative A-loops of small orders and also of order p^3, where p is a prime.

1. Introduction

A *loop* is a groupoid $(Q, \cdot)$ with neutral element 1 such that all left translations $L_x : Q \to Q$, $y \mapsto xy$ and all right translations $R_x : Q \to Q$, $y \mapsto yx$ are bijections of Q. Given a loop Q and x, $y \in Q$, we denote by $x \setminus y$ the unique element of Q satisfying $x \cdot x \setminus y = y$. In other words, $x \setminus y = L_x^{-1}(y)$.

To reduce the number of parentheses, we adopt the following convention for term evaluation: $\setminus$ is less binding than juxtaposition, and $\cdot$ is less binding than $\setminus$. For instance $xy \setminus u \cdot v \setminus w$ is parsed as $((xy) \setminus u)(v \setminus w)$.

The *inner mapping group* $\mathrm{Inn}(Q)$ of a loop Q is the permutation group generated by

$$L_{x,y} = L_{yx}^{-1} L_y L_x, \quad R_{x,y} = R_{xy}^{-1} R_y R_x, \quad T_x = L_x^{-1} R_x,$$

where x, $y \in Q$. A subloop of Q is *normal* if it is invariant under all inner mappings of Q.

A loop Q is an *automorphic loop* (or *A-loop*) if $\mathrm{Inn}(Q) \leq \mathrm{Aut}(Q)$, that is, if every inner mapping of Q is an automorphism of Q. Hence a commutative loop is an A-loop if all its left inner mappings $L_{yx}^{-1} L_y L_x$ are automorphisms, which can be expressed by the identity

$$xy \setminus x(yu) \cdot xy \setminus x(yv) = xy \setminus x(y \cdot uv). \tag{A}$$

Note that the class of commutative A-loops contains commutative groups and commutative Moufang loops.

We assume that the reader is familiar with the terminology and notation of loop theory, cf. [1] or [10]. This paper is a companion to [6], where we have presented a historical introduction and many new structural results concerning commutative *A*-loops, including:

- commutative A-loops are power-associative (cf. [2]),
- for a prime p, a finite commutative A-loop Q has order a power of p if and only if every element of Q has order a power of p,
- every finite commutative A-loop is a direct product of a loop of odd order (consisting of elements of odd order) and a loop of order a power of 2,
- commutative A-loops of odd order are solvable,
- the Lagrange and Cauchy theorems hold for commutative A-loops,
- every finite commutative A-loop has Hall π-subloops (and hence Sylow p-subloops),

2000 *Mathematics Subject Classification.* 20N05.

Key words and phrases. commutative automorphic loop, commutative A-loop, automorphic inner mappings, central extensions, enumeration of A-loops.

Přemysl Jedlička supported by the Grant Agency of the Czech Republic, grant no. 201/07/P015.

- if there is a nonassociative finite simple commutative A-loop, it is of exponent 2.

Despite these deep results, the theory of commutative A-loops is in its infancy. As an illustration of this fact, the present theory is not sufficiently developed to classify commutative A-loops of order 8 without the aid of a computer, commutative A-loops of order pq (where $p < q$ are primes), nor commutative A-loops of order p^3 (where p is a prime).

The two main problems for commutative A-loops stated in [6] were: *For an odd prime p, is every commutative A-loop of order p^k centrally nilpotent? Is there a nonassociative finite simple commutative A-loop, necessarily of exponent 2 and order a power of 2?* For an example of a commutative A-loop of order 8 that is not centrally nilpotent, see Subsection 3.1.

In the meantime, we have managed to solve the first problem of [6] in the affirmative, but we neither use nor prove the result here—it will appear elsewhere. The second problem remains open and the many constructions of commutative A-loops of exponent 2 obtained here can be seen as a step toward solving it.

One of the most important concepts in the investigation of commutative A-loops appears to be the middle nucleus $N_\mu(Q)$, since, by [2], $N_\lambda(Q) \leq N_\mu(Q)$, $N_\rho(Q) \leq N_\mu(Q)$ and $N_\mu(Q) \trianglelefteq Q$ is true in any A-loop Q. In §2 we characterize all commutative loops with middle nucleus of index 2, solve the isomorphism problem, and then characterize all commutative A-loops with middle nucleus of index 2. In §3 we classify commutative A-loops of order 8, among other applications of §2.

Central extensions of commutative A-loops are described in §4. A broad class of such extensions is obtained from trilinear forms that are symmetric with respect to an interchange of (fixed) two arguments. As an application, we characterize all parameters (k, ℓ) with the property that there is a nonassociative commutative A-loop of order 2^k with middle nucleus of order $2^\ell > 1$.

§5 uses another class of central extensions partially based on the overflow in modular arithmetic that yields many (conjecturally, all) nonassociative commutative A-loops of order p^3, where p is an odd prime.

A classification of commutative A-loops of small orders based on the theory and computer computations can be found in §6.

2. Commutative loops with middle nucleus of index 2

Throughout this section, we denote by $\overline{X} = \{\overline{x};\ x \in X\}$ a disjoint copy of the set X.

Let G be a commutative group and f a bijection of G. Then $G(f)$ will denote the groupoid $(G \cup \overline{G}, *)$ with multiplication

$$x * y = xy, \quad x * \overline{y} = \overline{xy}, \quad \overline{x} * y = \overline{xy}, \quad \overline{x} * \overline{y} = f(xy), \tag{2.1}$$

for x, $y \in G$. Note that $G(f)$ is a loop with neutral element 1.

Lemma 2.1. *Let G be a commutative group, f a bijection of G and $(Q, \cdot) = G(f) = (G \cup \overline{G}, *)$. Then:*

(i) *Q is commutative.*
(ii) *$x \setminus y = x^{-1}y$, $x \setminus \overline{y} = \overline{x^{-1}y}$, $\overline{x} \setminus y = \overline{x^{-1}f^{-1}(y)}$, $\overline{x} \setminus \overline{y} = x^{-1}y$ for every x, $y \in G$.*
(iii) *$G \leq N_\mu(Q)$.*
(iv) *Q is a group if and only if f is a translation of the group G.*
(v) *If Q is not a group (that is, $G = N_\mu(Q)$) then $N_\lambda(Q) = N_\rho(Q) = Z(Q) = \{x \in G;\ f(x) = xf(1)\}$.*

Proof. Part (i) follows from the definition of $G(f)$. Part (ii) is straightforward, for instance, $x * \overline{x^{-1}y} = \overline{xx^{-1}y} = \overline{y}$ shows that $x \setminus \overline{y} = \overline{x^{-1}y}$.

For (iii), let x, y, $z \in G$ and verify that

$$\begin{aligned} &x*(y*z) = (x*y)*z,\\ &\overline{x}*(y*z) = \overline{x}*yz = \overline{xyz} = \overline{xy}*z = (\overline{x}*y)*z,\\ &x*(y*\overline{z}) = x*\overline{yz} = \overline{xyz} = xy*\overline{z} = (x*y)*\overline{z},\\ &\overline{x}*(y*\overline{z}) = \overline{x}*\overline{yz} = f(xyz) = \overline{xy}*\overline{z} = (\overline{x}*y)*\overline{z}. \end{aligned}$$

This shows $G \leq N_\mu(Q)$.

(iv) An easy calculation shows that $\overline{1} \in N_\mu(Q)$ (that is, Q is a group) if and only if $f(xy) = xf(y) = f(x)y$ for every x, $y \in G$. With $y = 1$ we deduce that $f(x) = xf(1)$ for every x. On the other hand, $f(x) = xf(1)$ implies $f(xy) = xf(y) = f(x)y$.

(v) Let x, y, $z \in G$. Then $x*(y*z) = (x*y)*z$, $x*(\overline{y}*z) = \overline{xyz} = (x*\overline{y})*z$, $x*(y*\overline{z}) = \overline{xyz} = (x*y)*\overline{z}$, and $x*(\overline{y}*\overline{z}) = xf(yz)$ while $(x*\overline{y})*\overline{z} = f(xyz)$. Hence $x \in N_\lambda(Q)$ if and only if $xf(yz) = f(xyz)$ for every y, $z \in G$. With $y = z = 1$, this condition reduces to $f(x) = xf(1)$. On the other hand, $f(x) = xf(1)$ already implies $xf(yz) = xyzf(1) = f(xyz)$. We have $N_\rho(Q) = N_\lambda(Q)$ by commutativity of $*$. Since our assumption is $G = N_\mu(Q)$, we conclude that $N_\lambda(Q) = N_\rho(Q) = Z(Q) = \{x \in G;\ f(x) = xf(1)\}$. □

Lemma 2.2. *Let Q be a commutative loop with subloop G satisfying $G \leq N_\mu(Q)$, $[Q : G] = 2$. Then G is a commutative group and there exists a bijection f of G such that Q is isomorphic to $G(f)$.*

Proof. The commutative loop G is a group by $G \leq N_\mu(Q)$. Denote by $\overline{1}$ a fixed element of $Q \setminus G$, and define $\overline{x} = \overline{1}x = x\overline{1}$ for every $x \in G$. Note that $\overline{1}$ is well-defined, $G \cap \overline{G} = \emptyset$ and $Q = G \cup \overline{G}$. Moreover, $x\overline{y} = x \cdot y\overline{1} = xy \cdot \overline{1} = \overline{xy}$ and $\overline{x}y = \overline{1}x \cdot \overline{y} = \overline{1} \cdot xy = \overline{xy}$ for every x, $y \in G$, using $G \leq N_\mu(Q)$ again. Finally, if x_1, y_1, x_2, $y_2 \in G$ satisfy $x_1y_1 = x_2y_2$ then

$$\overline{x_1y_1} = \overline{1}x_1 \cdot y_1\overline{1} = \overline{1}(x_1 \cdot y_1\overline{1}) = \overline{1}(x_1y_1 \cdot \overline{1}) = \overline{1}(x_2y_2 \cdot \overline{1}) = \overline{x_2y_2}.$$

Thus the multiplication in the quadrant $\overline{G} \times \overline{G}$ mimics that of $G \times G$, except that the elements are renamed according to the permutation $f : G \to G$, $x \mapsto \overline{1} \cdot x\overline{1}$. □

Corollary 2.3. *Let Q be a commutative loop. Then $[Q : N_\mu(Q)] \leq 2$ if and only if there exists a commutative group G and a bijection f of G such that Q is isomorphic to $G(f) = (G \cup \overline{G}, *)$ defined by* (2.1).

We now solve the isomorphism problem for nonassociative commutative loops with middle nucleus of index 2 in terms of the associated bijections:

Proposition 2.4. *Let G be a commutative group and f_1, f_2 bijections of G such that $G(f_1)$, $G(f_2)$ are not groups. Then $G(f_1) \cong G(f_2)$ if and only if there is $\psi \in \mathrm{Aut}(G)$ such that*

$$f_2^{-1}\psi f_1(x) = f_2^{-1}\psi f_1(1) \cdot \psi(x) \quad \text{for all } x \in G, \tag{2.2}$$

and $f_2^{-1}\psi f_1(1)$ is a square in G.

Proof. Denote by $*$ the multipication in $G(f_1)$, and by $\circ$ the multiplication in $G(f_2)$.

Assume that $\varphi : G(f_1) \to G(f_2)$ is an isomorphism. Since $G(f_1)$, $G(f_2)$ are not groups, φ maps $N_\mu(G(f_1)) = G$ onto $N_\mu(G(f_2)) = G$, and hence $\psi = \varphi|_G$ is a bijection of G. Then

$$\psi(xy) = \varphi(xy) = \varphi(x*y) = \varphi(x) \circ \varphi(y) = \psi(x) \circ \psi(y) = \psi(x)\psi(y)$$

for every x, $y \in G$, so $\psi \in \mathrm{Aut}(G)$.

Define $\rho : G \to G$ by $\overline{\rho(x)} = \varphi(\overline{x})$. We have

$$\overline{\rho(x)} = \varphi(\overline{x}) = \varphi(x*\overline{1}) = \varphi(x) \circ \varphi(\overline{1}) = \psi(x) \circ \overline{\rho(1)} = \overline{\psi(x)\rho(1)},$$

so $\rho(x) = \rho(1)\psi(x)$ for every $x \in G$. Using this observation, we have

$$\psi(f_1(xy)) = \varphi(f_1(xy)) = \varphi(\overline{x}*\overline{y}) = \varphi(\overline{x})\circ\varphi(\overline{y}) = \overline{\rho(x)}\circ\overline{\rho(y)} = f_2(\rho(x)\rho(y)) = f_2(\rho(1)^2\psi(xy)).$$

Equivalently, $f_2^{-1}\psi f_1(x) = \rho(1)^2\psi(x)$ for every $x \in G$. With $x = 1$, we deduce that $\rho(1)^2 = f_2^{-1}\psi f_1(1)$ is a square, and that (2.2) holds.

Conversely, assume that (2.2) holds for some $\psi \in \mathrm{Aut}(G)$, and that $u^2 = f_2^{-1}\psi f_1(1)$ is a square in G. Define $\varphi : G(f_1) \to G(f_2)$ by $\varphi(x) = \psi(x)$, $\varphi(\overline{x}) = \overline{u\psi(x)}$. Then

$$\varphi(x * y) = \varphi(xy) = \psi(xy) = \psi(x)\psi(y) = \psi(x) \circ \psi(y) = \varphi(x) \circ \varphi(y),$$
$$\varphi(\overline{x} * y) = \varphi(\overline{xy}) = \overline{u\psi(xy)} = \overline{u\psi(x)\psi(y)} = \overline{u\psi(x)} \circ \psi(y) = \varphi(\overline{x}) \circ \varphi(y),$$

and, similarly, $\varphi(x * \overline{y}) = \varphi(x) \circ \varphi(\overline{y})$ for every x, $y \in G$. Finally, using (2.2) to obtain the third equality below, we have

$$\varphi(\overline{x} * \overline{y}) = \varphi(f_1(xy)) = \psi(f_1(xy)) = f_2(u^2\psi(xy)) = \overline{u\psi(x)} \circ \overline{u\psi(y)} = \varphi(\overline{x}) \circ \varphi(\overline{y})$$

for every x, $y \in G$. Thus $G(f_1) \cong G(f_2)$. □

We say that two bijections f_1, f_2 of G are *conjugate in* $\mathrm{Aut}(G)$ if there is $\psi \in \mathrm{Aut}(G)$ such that $f_2 = \psi f_1 \psi^{-1}$. The following specialization of Proposition 2.4 will be useful in the classification of commutative A-loops of order 8.

Corollary 2.5. *Let G be a commutative group, and let f_1, f_2 be bijections of G such that $G(f_1)$, $G(f_2)$ are not groups.*

(i) *If f_1, f_2 are conjugate in $\mathrm{Aut}(G)$ then $G(f_1) \cong G(f_2)$.*
(ii) *If $f_1(1) = 1 = f_2(1)$ then $G(f_1) \cong G(f_2)$ if and only if f_1, f_2 are conjugate in $\mathrm{Aut}(G)$.*
(iii) *If $f_2 \in \mathrm{Aut}(G)$, t is a square in G and $f_1(x) = f_2(x)t$ for every $x \in G$ then $G(f_1) \cong G(f_2)$.*

Proof. (i) Let $\psi \in \mathrm{Aut}(G)$ be such that $f_2 = \psi f_1 \psi^{-1}$. Then $f_2^{-1}\psi f_1 = \psi f_1^{-1}\psi^{-1}\psi f_1 = \psi$, so $f_2^{-1}\psi f_1(1) = \psi(1) = 1$ is a square and (2.2) holds.

(ii) Assume that $G(f_1) \cong G(f_2)$. Then there is $\psi \in \mathrm{Aut}(G)$ such that (2.2) holds. Since $f_2^{-1}\psi f_1(1) = f_2^{-1}\psi(1) = f_2^{-1}(1) = 1$, we deduce from (2.2) that f_1, f_2 are conjugate in $\mathrm{Aut}(G)$. The converse follows by (i).

(iii) Let ψ be the trivial automorphism of G. Then (2.2) becomes $f_2^{-1}f_1(x) = f_2^{-1}f_1(1) \cdot x$, and it is our task to check this identity and that $f_2^{-1}f_1(1)$ is a square. Now, $f_2^{-1}f_1(1) = f_2^{-1}(f_2(1)t) = f_2^{-1}(f_2(1))f_2^{-1}(t) = f_2^{-1}(t)$ is a squares since t is. Moreover, $f_1(1) = f_2(1)\cdot t = t$, so $f_1(x) = f_1(1)f_2(x)$, and (2.2) follows upon applying f_2^{-1} to this equality. □

Finally, we describe all commutative A-loops with middle nucleus of index 2.

Proposition 2.6. *The following conditions are equivalent for a commutative loop Q possessing a subgroup of index 2:*

(i) *Q is an A-loop and $[Q : N_\mu(Q)] \leq 2$.*
(ii) *$Q = G(f)$, where G is a commutative group, $[Q : G] = 2$, and f is a permutation of G satisfying*

$$f(xy) = f(x)f(y)f(1)^{-1}, \tag{P_1}$$
$$f(x^2) = x^2 f(1), \tag{P_2}$$
$$f^2(x)^2 f(x)^{-2} = f^2(1) \tag{P_3}$$

for every x, $y \in G$.
(iii) *$Q = G(f)$, where G is a commutative group, $[Q : G] = 2$, and f is a permutation of G satisfying (P_1), (P_2) and $f^2(1) = f(1)^2$.*

(iv) $Q = G(f)$, *where* G *is a commutative group,* $[Q : G] = 2$, $f(x) = g(x)t$ *for every* $x \in G$, $g \in \mathrm{Aut}(G)$, $g(x^2) = x^2$ *for every* $x \in G$, *and* t *is a fixed point of* g.

Proof. By Corollary 2.3, we can assume that $Q = G(f) = (G \cup \overline{G}, *)$, where $G \leq N_\mu(Q)$ is a commutative group and f is a bijection of G. (The global assumption that Q possesses a subgroup of index 2 is needed only in (i) when Q is a group, to guarantee the existence of G.) Let us establish the equivalence of (i) and (ii).

Denote by $\alpha(a, b, c, d)$ the $*$ version of (A), namely

$$(a * b) \setminus (a * (b * (c * d))) = [(a * b) \setminus (a * (b * c))] * [(a * b) \setminus (a * (b * d))],$$

where a, b, c, d are taken from $G \cup \overline{G}$. With the exception of the variables a, b, c, d, we implicitly assume that variables without bars are taken from G, while variables with bars are taken from $\overline{G}$.

Then $\alpha(x, y, u, v)$ holds, as the evaluation of $\alpha(x, y, u, v)$ takes place in the group G. Since $y \in N_\mu(Q)$, $\alpha(a, y, c, d)$ holds. By commutativity of $*$, $\alpha(a, b, c, d)$ holds if and only if $\alpha(a, b, d, c)$ holds. Hence it remains to investigate the identities $\alpha(x, \overline{y}, u, v)$, $\alpha(x, \overline{y}, u, \overline{v})$, $\alpha(x, \overline{y}, \overline{u}, \overline{v})$, $\alpha(\overline{x}, \overline{y}, u, v)$, $\alpha(\overline{x}, \overline{y}, u, \overline{v})$, and $\alpha(\overline{x}, \overline{y}, \overline{u}, \overline{v})$.

Straightforward calculation with (2.1) and Lemma 2.1 shows that $\alpha(\overline{x}, \overline{y}, u, \overline{v})$ holds if and only if

$$xf(yuv) = f(xy)^{-1} f(xyu) xf(yv). \tag{2.3}$$

Using $x = y = 1$, (2.3) reduces to (P_1). On the other hand, (P_1) already implies (2.3), and so $\alpha(\overline{x}, \overline{y}, u, \overline{v})$ is equivalent to (P_1). From now on, we will assume that (P_1) holds and denote $f(1)$ by t.

The identity $\alpha(x, \overline{y}, \overline{u}, \overline{v})$ is then equivalent to

$$x^{-1}t^{-1} = f(x^{-2}) f(y^{-2}) f(y)^2 x t^{-5}, \tag{2.4}$$

and since $t = f(yy^{-1}) = f(y)f(y^{-1})t^{-1}$ yields

$$f(y^{-1}) = f(y)^{-1} t^2, \tag{2.5}$$

we can rewrite (2.4) as $f(x)^2 = x^2 t^2$, or, equivalently (using (P_1)), as (P_2).

Finally, note that (P_1) and (2.5) imply

$$f^2(uv) = f(f(uv)) = f(f(u)f(v)t^{-1}) = f^2(u) f^2(v) f(t^{-1}) t^{-2} = f^2(u) f^2(v) f(t)^{-1}. \tag{2.6}$$

Using (2.6) and (2.5), we see, after a lengthy calculation, that the identity $\alpha(\overline{x}, \overline{y}, \overline{u}, \overline{v})$ is equivalent to (P_3).

We leave it to the reader to check that the identities $\alpha(x, \overline{y}, u, v)$, $\alpha(x, \overline{y}, u, \overline{v})$, $\alpha(x, \overline{y}, \overline{u}, \overline{v})$ imply no additional conditions on f beside (P_1)–(P_3), and, conversely, that if (P_1)–(P_3) are satisfied then the identities $\alpha(x, \overline{y}, u, v)$, $\alpha(x, \overline{y}, u, \overline{v})$, $\alpha(x, \overline{y}, \overline{u}, \overline{v})$ hold.

We have proved the equivalence of (i) and (ii).

Assume that (ii) holds. With $x = 1$ in (P_3) we have $f^2(1)^2 f(1)^{-2} = f(t)$, or $f(t)^2 t^{-2} = f(t)$, or $f(t) = t^2$, so (iii) holds. Conversely, assume that (iii) holds. Then, $f^2(x)^2 f(t)^{-1} = f^2(x) t^{-2} = f(f(x)) f(f(x)) t^{-2} = f(f(x)f(x)) t^{-1} = f(f(x)^2) t^{-1} = f(x)^2$, which is (P_3), so (ii) holds.

Assume that (iii) holds and define g by $g(x) = f(x)t^{-1}$, where $t = f(1)$. Then $g(xy) = f(xy)t^{-1} = f(x)f(y)t^{-2} = f(x)t^{-1}f(y)t^{-1} = g(x)g(y)$ by (P_1), $g(x^2) = f(x^2)t^{-1} = x^2$ by (P_2), and $g(t) = f(t)t^{-1} = t$ by $f(t) = t^2$. Conversely, assume that (iv) holds, $f(x) = g(x)t$, $g \in \mathrm{Aut}(G)$, where t is a fixed point of g (not necessarily satisfying $t = f(1)$). Then $f(1) = g(1)t = t$, $f(xy) = g(xy)t = g(x)g(y)t = g(x)tg(y)tt^{-1} = f(x)f(y)t^{-1}$, $f(x^2) = g(x^2)t = x^2 t$, and $f(t) = g(t)t = t^2$, proving (iii). □

3. Constructions of commutative A-loops with middle nucleus of index 2

As an application of Proposition 2.6, we classify all commutative A-loops of order 8 and present a class of commutative A-loops of exponent 2 with trivial center and middle nucleus of index 2.

3.1. **Commutative A-loops of order 8.** It is not difficult to classify all commutative A-loops of order 8 up to isomorphism with a finite model builder, such as Mace4 [7]. It turns out that there are 4 nonassociative commutative A-loops of order 8. All such loops have middle nucleus of index 2; a fact for which we do not have a human proof. But using this fact, we can finish the classification by hand with Proposition 2.4, Corollary 2.5 and Proposition 2.6.

Lemma 3.1. *Let G be a commutative loop, $g \in \mathrm{Aut}(G)$ and $t \in G$. Let f be a bijection of G defined by $f(x) = g(x)t$. Then $Z(G(f)) = Z(G(g))$ as sets.*

Proof. If $1 = g$ then f is a translation by t and both $G(g)$, $G(f)$ are commutative groups, hence $Z(G(g)) = G \cup \overline{G} = Z(G(f))$.

Assume that $1 \neq g$. Then neither g nor f is a translation of G, so both $G(g)$ and $G(f)$ are nonassociative, by Lemma 2.1(iv). By Lemma 2.1(v), $Z(G(f)) = \{x \in G;\ f(x) = xf(1)\} = \{x \in G;\ g(x)t = xt\} = \{x \in G;\ g(x) = x\} = Z(G(g))$. □

Let Q be a nonassociative commutative A-loop of order 8, necessarily with a middle nucleus of index 2. By Proposition 2.6, $Q = G(f)$, where G is a commutative group of order 4 and $f(x) = g(x)t$ for some $g \in \mathrm{Aut}(G)$ and $t \in G$ such that $g(x^2) = x^2$ and $g(t) = t$.

Let $G = \mathbb{Z}_4 = \langle a \rangle$ be the cyclic group of order 4. The two automorphisms of G are the trivial automorphism $g = 1$ and the transposition $g = (a, a^3)$; both fix all squares of G. Let $g = 1$ and $f(x) = g(x)t$ for some $t \in G$. Then $G(f)$ is a commutative group by Lemma 2.1(v). Assume that $g = (a, a^3)$. Then $G(g)$ is a nonassociative commutative A-loop. The only nontrivial fixed point of g is a^2. Let $f(x) = g(x)a^2$. By Corollary 2.5(iii), $G(f) \cong G(g)$.

Now let $G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \langle a \rangle \times \langle b \rangle$ be the Klein group. Then $\mathrm{Aut}(G) = \{(),\ (a, b),\ (a, ab),\ (b, ab),\ (a, b, ab),\ (a, ab, b)\} \cong S_3$. The only square in G is 1 and it is trivially fixed by all $g \in \mathrm{Aut}(G)$.

If $g = 1$ and $f(x) = g(x)t$ for some $t \in G$, $G(g)$ is a commutative group by Lemma 2.1(v). Assume that $g_1 = (a, b)$. The choices for t are $t = 1$, $t = ab$. Let $f_1(x) = g_1(x)ab$. Then $G(g_1)$, $G(f_1)$ are nonassociative commutative A-loops. Since $g_1(xx) = g_1(1) = 1$, $G(g_1)$ has exponent 2. Since $f_1(xx) = f_1(1) = ab$, $G(f_1)$ does not have exponent 2. Hence $G(g_1) \ncong G(f_1)$.

Assume that $g_2 = (a, ab)$, and note that the choices for t are $t = 1$, $t = b$. Let $f_2(x) = g_2(x)b$. Since all transpositions of S_3 are conjugate in S_3, $G(g_1) \cong G(g_2)$ by Corollary 2.5(i). Note that $f_1 = \psi^{-1} f_2 \psi$ with $\psi = (b, ab)$. Hence $G(f_1) \cong G(f_2)$ by Corollary 2.5.

Similarly, no new nonassociative commutative A-loop of order 8 is obtained with $g_3 = (b, ab)$.

Let $g_4 = (a, b, ab)$. Then $t = 1$ is the only choice, and $G(g_4)$ is a nonassociative commutative A-loop. By Lemma 2.1(v), $Z(G(g_4)) = 1$ and $Z(G(g_1)) \cong \mathbb{Z}_2$. By Lemma 3.1, $Z(G(f_1)) \cong Z(G(g_1))$. Thus $G(g_4)$ is a new nonassociative commutative A-loop.

Finally, let $g_5 = (a, ab, b)$. Since g_4, g_5 are conjugate in $\mathrm{Aut}(G)$, $G(g_4) \cong G(g_5)$ by Corollary 2.5(i).

3.2. **A class of commutative A-loops of exponent 2 with trivial center and middle nucleus of index 2.** Let GF(2) be the two-element field and let V be a vector space over GF(2) of dimension $n \geq 2$. Let $G = (V, +)$ be the corresponding elementary abelian 2-group.

Let $\{e_1, \ldots, e_n\}$ be a basis of V. Define an automorphism of G by

$$g(e_1) = e_2, \quad g(e_2) = e_3, \quad g(e_{n-1}) = e_n, \quad g(e_n) = e_1 + e_n.$$

Since $g(x+x) = g(0) = 0 = g(x) + g(x)$, Proposition 2.6 with $f = g$ shows that $Q_n = G(f)$ is a commutative A-loop of order 2^{n+1} with nucleus of index at most 2.

We claim that g has no fixed points besides 0. Indeed, for $x = \sum_{i=1}^{n} \alpha_i e_i$ we have

$$g(x) = \alpha_n e_1 + \alpha_1 e_2 + \cdots \alpha_{n-2} e_{n-1} + (\alpha_{n-1} + \alpha_n) e_n,$$

so $x = g(x)$ if and only if

$$\alpha_1 = \alpha_n, \quad \alpha_2 = \alpha_1, \quad \alpha_{n-1} = \alpha_{n-2}, \quad \alpha_n = \alpha_{n-1} + \alpha_n,$$

or, $\alpha_1 = \cdots = \alpha_n = 0$.

Thus Lemma 2.1(v) implies that Q_n has trivial center. In particular, Q_n is not a group, and $[Q_n : N_\mu(Q_n)] = 2$ follows. Finally, $x * x = x + x = 0$ and $\overline{x} * \overline{x} = g(x+x) = 0$ for every $x \in G$, so Q_n has exponent two.

4. Central extensions based on trilinear forms

Let Z, K be loops. We say that a loop Q is an *extension* of Z by K if $Z \trianglelefteq Q$ and $Q/Z \cong K$. If $Z \leq Z(Q)$, the extension is said to be *central*.

It is well-known that central extensions of an abelian group Z by a loop K are precisely the loops $K \ltimes_\theta Z$ defined on $K \times Z$ by

$$(x, a)(y, b) = (xy,\ ab\theta(x, y)),$$

where $\theta : K \times K \to Z$ is a *(loop) cocycle*, that is, a mapping satisfying $\theta(x, 1) = \theta(x, 1) = 1$ for every $x \in K$.

In [2, Theorem 6.4], Bruck and Paige described all central extensions of an abelian group Z by an A-loop K resulting in an A-loop Q. The cocycle identity they found is rather complicated, and despite some optimism of Bruck and Paige, it is by no means easy to construct cocycles that conform to it.

In the commutative case, we deduce from [2, Theorem 6.4]:

Corollary 4.1. *Let Z be an abelian group and K a commutative A-loop. Let $\theta : K \times K \to Z$ be a cocycle satisfying $\theta(x, y) = \theta(y, x)$ for every x, $y \in K$ and*

$$F(x, y, z)F(x', y, z)\theta(R_{y,z}(x), R_{y,z}(x')) = F(xx', y, z)\theta(x, x') \tag{4.1}$$

for every x, y, z, $x' \in K$, where

$$F(x, y, z) = \theta(R_{y,z}(x), yz)^{-1}\theta(y, z)^{-1}\theta(xy, z)\theta(x, y).$$

Then $K \ltimes_\theta Z$ is a commutative A-loop.

Conversely, every commutative A-loop that is a central extension of Z by K can be represented in this manner.

Corollary 4.2. *Let Z be an elementary abelian 2-group and K a commutative A-loop of exponent two. Let $\theta : K \times K \to Z$ be a cocycle satisfying $\theta(x, y) = \theta(y, x)$ for every x, $y \in K$, $\theta(x, x) = 1$ for every $x \in K$, and*

$$\theta(x, y)\theta(x', y)\theta(xx', y)\theta(x, x')\theta(xy, z)\theta(x'y, z)\theta(y, z)\theta((xx')y, z) = \\ \theta(R_{y,z}(x), yz)\theta(R_{y,z}(x'), yz)\theta(R_{y,z}(xx'), yz)\theta(R_{y,z}(x), R_{y,z}(x')) \tag{4.2}$$

for every x, y, z, $x' \in K$. Then $K \ltimes_\theta Z$ is a commutative A-loop of exponent two.

Conversely, every commutative A-loop of exponent two that is a central extension of Z by K can be represented in this manner.

When K is an elementary abelian 2-group, the cocycle identity (4.2) can be rewritten as

$$\begin{aligned}&\theta(x,y)\theta(x',y)\theta(xx',y)\\&\theta(xy,z)\theta(x'y,z)\theta(xx',z)\\&\theta(x,yz)\theta(x',yz)\theta(xx',yz)\\&\theta(y,z)\theta(xx',z)\theta((xx')y,z)=1.\end{aligned}\tag{4.3}$$

Since every line above is of the form $\theta(u,w)\theta(v,w)\theta(uv,w)$, it is tempting to try to satisfy (4.2) by imposing $\theta(u,w)\theta(v,w)\theta(uv,w)=1$ for every $u,\ v,\ w\in K$. However, that identity already implies associativity. A nontrivial solution to the cocycle identity for commutative A-loops of exponent two can be obtained as follows:

Proposition 4.3. *Let $Z=\mathrm{GF}(2)$ and let K be an elementary abelian 2-group. Let $g: K^3\to\mathrm{GF}(2)$ be a trilinear form such that $g(x,xy,y)=g(y,xy,x)$ for every $x,\ y\in K$. Define $\theta: K^2\to\mathrm{GF}(2)$ by $\theta(x,y)=g(x,xy,y)$. Then $Q=K\ltimes_\theta Z$ is a commutative A-loop of exponent 2. Moreover, $(y,b)\in N_\mu(Q)$ if and only if for every $x,\ z\in K$ we have $g(y,x,z)=g(x,z,y)$.*

Proof. Trilinearity alone implies that $\theta(u,w)\theta(v,w)\theta(uv,w)=g(u,v,w)g(v,u,w)$. The left-hand side of (4.3) can then be rewritten as

$$g(x,x',y)g(x',x,y)g(xy,x'y,z)g(x'y,xy,z)g(x,x',yz)g(x',x,yz)g(y,xx',z)g(xx',y,z),$$

which reduces to 1 by trilinearity.

We have $(y,b)\in N_\mu(Q)$ if and only if $\theta(x,y)\theta(xy,z)=\theta(y,z)\theta(x,yz)$ for every $x,\ z\in K$, and the rest follows from trilinearity of g. □

Let $V=\mathrm{GF}(2)^n$. Call a 3-linear form $g: V\to\mathrm{GF}(2)$ $(1,3)$-*symmetric* if $g(x,y,z)=g(z,y,x)$ for every $x,\ y,\ z\in V$. By Proposition 4.3, a $(1,3)$-symmetric trilinear form gives rise to a commutative A-loop Q of exponent 2, and $(y,b)\in N_\mu(Q)$ if and only if $g(y,x,z)=g(y,z,x)$, that is, if and only if the induced bilinear form $g(y,-,-):V^2\to\mathrm{GF}(2)$ is symmetric.

Example 4.4. *Let $V=\mathrm{GF}(2)^3$ with basis $\{e_1,e_2,e_3\}$. Define a $(1,3)$-symmetric trilinear form $g: V^3\to\mathrm{GF}(2)$ by $g(e_i,e_j,e_k)=0$ for every $1\le i,\ j,\ k\le 3$, except for $g(e_1,e_2,e_1)=g(e_2,e_1,e_3)=g(e_3,e_2,e_3)=1$. Then it is not difficult to check (by computer) that for every $0\neq x\in V$ the induced form $g(x,-,-):V^2\to\mathrm{GF}(2)$ is not symmetric.*

Lemma 4.5. *Let $V=\mathrm{GF}(2)^n$, $n\ge 3$. Then there is a $(1,3)$-symmetric form $g: V^3\to\mathrm{GF}(2)$ such that for every $0\neq x\in V$ the induced bilinear form $g(x,-,-)$ is not symmetric.*

Proof. We proceed by induction on n. When $n=3$, see Example 4.4. Assume that V has basis $\{e_1,\dots,e_{n+1}\}$, and that for the hyperplane $W=\langle e_1,\dots,e_n\rangle$ we have a $(1,3)$-symmetric form $g: W^3\to\mathrm{GF}(2)$ such that for every $0\neq x\in W$ the induced form $g(x,-,-)$ is not symmetric. Extend g into a $(1,3)$-symmetric trilinear form $\widehat{g}: V^3\to\mathrm{GF}(2)$ arbitrarily but subject to the restrictions

$$\begin{aligned}&\widehat{g}(e_{n+1},e_i,e_j)=g(e_n,e_i,e_j)\text{ for }1\le i,\ j\le n,\\&\widehat{g}(e_{n+1},e_n,e_{n+1})\neq\widehat{g}(e_{n+1},e_{n+1},e_n),\\&\widehat{g}(e_n,e_{n+1},e_n)=\widehat{g}(e_{n+1},e_n,e_n).\end{aligned}$$

For $0\neq x\in W$ the induced form $\widehat{g}(x,-,-)$ is an extension of the form $g(x,-,-)$, and hence it is not symmetric. Furthermore, $\widehat{g}(e_{n+1}+x,y,z)=\widehat{g}(e_{n+1},y,z)+g(x,y,z)=g(e_n,y,z)+g(x,y,z)=g(e_n+x,y,z)$, so $\widehat{g}(e_{n+1}+x,-,-)$ is not symmetric as long as $x\neq e_n$. By definition, $\widehat{g}(e_{n+1}+e_n,e_n,e_{n+1})=\widehat{g}(e_{n+1},e_n,e_{n+1})+\widehat{g}(e_n,e_n,e_{n+1})=\widehat{g}(e_{n+1},e_n,e_{n+1})+\widehat{g}(e_{n+1},e_n,e_n)\neq$

$\widehat{g}(e_{n+1}, e_{n+1}, e_n) + \widehat{g}(e_n, e_{n+1}, e_n) = \widehat{g}(e_{n+1} + e_n, e_{n+1}, e_n)$, so $\widehat{g}(e_{n+1} + e_n, -, -)$ is not symmetric. Finally, $\widehat{g}(e_{n+1}, -, -)$ is not symmetric on $\langle e_n, e_{n+1}\rangle$ by definition. □

Example 4.6. *By Lemma 4.5, for every $n \geq 3$ there is a commutative A-loop Q of exponent 2 and order 2^{n+1} with $N_\mu(Q) = Z(Q)$, $|Z(Q)| = 2$.*

Let Q be a finite commutative A-loop of exponent 2. By results of [6], $|Q| = 2^k$ for some k. Let $|N_\mu(Q)| = 2^\ell$. We show how to realize all possible pairs (k, ℓ) with $\ell > 0$.

Lemma 4.7. *Let $k \geq \ell > 0$. Then there is a nonassociative commutative A-loop of order 2^k with middle nucleus of order 2^ℓ if and only if: either $d = k - \ell \geq 3$, or $d \geq 1$ and $\ell \geq 2$.*

Proof. If $d \geq 3$, consider the loop Q of order 2^{d+1} with middle nucleus of order 2 from Example 4.6. Then $Q \times (\mathbb{Z}_2)^{k-d+1}$ achieves the parameters (k, ℓ).

Assume that $d = 2$. The parameters $(3, 1)$ are not possible by §3, and the parameters $(4, 2)$ are possible (see §6). Then (k, ℓ) can be achieved using the appropriate direct product.

Finally, assume that $d = 1$. Then we are done by Subsection 3.2. We obviously must have $\ell \geq 2$, else $|Q| = 2^k \leq 4$. □

We remark that Lemma 4.5 cannot be improved:

Lemma 4.8. *Let $V = \mathrm{GF}(2)^n$ and let $g : V^3 \to \mathrm{GF}(2)$ be a $(1, 3)$-symmetric trilinear form. If $n < 3$ then there is $0 \neq x \in V$ such that the induced form $g(x, -, -)$ is symmetric.*

Proof. There is nothing to show when $n = 1$, so assume that $n = 2$ and $\{e_1, e_2\}$ is a basis of V. The form g is determined by the 6 values $g(e_1, e_1, e_1)$, $g(e_1, e_1, e_2)$, $g(e_1, e_2, e_1)$, $g(e_1, e_2, e_2)$, $g(e_2, e_1, e_2)$ and $g(e_2, e_2, e_2)$.

Suppose that no induced form $g(x, -, -)$ is symmetric, for $0 \neq x \in V$. Then $g(e_1, e_1, e_2) \neq g(e_1, e_2, e_1)$, else $g(e_1, -, -)$ is symmetric. Similarly, $g(e_2, e_1, e_2) \neq g(e_2, e_2, e_1)$. But then $g(e_1 + e_2, e_1, e_2) = g(e_1, e_1, e_2) + g(e_2, e_1, e_2) = g(e_1, e_2, e_1) + g(e_2, e_2, e_1) = g(e_1 + e_2, e_2, e_1)$, hence $g(e_1 + e_2, -, -)$ is symmetric, a contradiction. □

Remark 4.9. *The many examples presented so far might suggest that $Q/N_\mu(Q)$ is a group in every commutative A-loop. This is not so: Consider a commutative Moufang loop Q. Then Q is a commutative A-loop, and $N_\mu(Q) = Z(Q)$ since the three nuclei of Q coincide. So the statement "$Q/N_\mu(Q)$ is a group" is equivalent to "$Q/Z(Q)$ is an abelian group", i.e., to "Q has nilpotency class at most 2". There are commutative Moufang loops of nilpotency class 3.*

Problem 4.10. *Find a smallest commutative A-loop Q in which $Q/N_\mu(Q)$ is not a group.*

4.1. **Adding group cocycles.** Let Z be an abelian group and K a loop. Then a loop cocycle $\theta : K \times K \to Z$ is said to be a *group cocycle* if it satisfies the identity

$$\theta(x, y)\theta(xy, z) = \theta(y, z)\theta(x, yz). \tag{4.4}$$

Note that if K is a group and θ is a group cocycle then $K \ltimes_\theta Z$ is a group, too.

Lemma 4.11. *Let Z be an abelian group, K a group and θ, $\mu : K \times K \to Z$ loop cocycles such that $\nu = \theta\mu^{-1} : (x, y) \mapsto \theta(x, y)\mu(x, y)^{-1}$ is a group cocycle. Then the left inner mappings in $K \ltimes_\theta Z$ and $K \ltimes_\mu Z$ coincide.*

Proof. Calculating in $K \ltimes_\theta Z$, we have

$$(x, a)(y, b) = (xy, ab\theta(x, y)),$$
$$(x, a) \setminus (y, b) = (x \setminus y, a^{-1}b\theta(x, x \setminus y)^{-1}).$$

Then

$$(x,a)(y,b)\setminus(x,a)((y,b)(z,c)) = (xy, ab\theta(x,y))\setminus(xyz, abc\theta(x,yz)\theta(y,z)$$
$$= (z, c\theta(x,yz)\theta(y,z)\theta(x,y)^{-1}\theta(xy,z)^{-1}). \quad (4.5)$$

Thus the left inner mappings in $K \ltimes_\theta Z$ and $K \ltimes_\mu Z$ coincide if and only if

$$\theta(x,yz)\theta(y,z)\theta(x,y)^{-1}\theta(xy,z)^{-1} = \mu(x,yz)\mu(y,z)\mu(x,y)^{-1}\mu(xy,z)^{-1}$$

for every x, y, $z \in K$, which happens precisely when $\nu = \theta\mu^{-1}$ is a group cocycle. □

Lemma 4.12. *Let Z be an abelian group, K a group and $\theta : K \times K \to Z$ a cocycle such that $K \ltimes_\theta Z$ is a commutative A-loop. Let $\mu : K \times K \to Z$ be a group cocycle satisfying $\mu(x,y) = \mu(y,x)$ for every x, $y \in K$. Then $K \ltimes_{\mu\theta} Z$ is a commutative A-loop with the same (left) inner mappings as $K \ltimes_\theta Z$.*

Proof. Both $Q_\theta = K \ltimes_\theta Z$, $Q_{\mu\theta} = K \ltimes_{\mu\theta} Z$ are commutative loops. Since $\mu\theta\theta^{-1}$ is a group cocycle, $Q_{\mu\theta}$ has the same (left) inner mappings as Q_θ, by Lemma 4.11. It therefore remains to show that every left inner mapping of $Q_{\mu\theta}$ is an automorphism.

Let (x,a), $(y,b) \in K \times Z$ and let φ be a left inner mapping of $Q_{\mu\theta}$ (and hence of Q_θ). Denote by $\cdot$ the multiplication in Q_θ and by $*$ the multiplication in $Q_{\mu\theta}$. Then

$$\varphi((x,a) * (y,b)) = \varphi((x,a)\cdot(y,b)\cdot(1,\mu(x,y))) = \varphi((x,a))\cdot\varphi((y,b))\cdot(1,\mu(x,y)),$$

because $(1,\mu(x,y)) \in Z$ is a central element. The equation (4.5) in fact shows that $\varphi((x,a)) = (x,a')$ for some a', and similarly, $\varphi((y,b)) = (y,b')$ for some b'. Thus

$$\varphi((x,a))\cdot\varphi((y,b))\cdot(1,\mu(x,y)) = (x,a')\cdot(y,b'0\cdot(1,\mu(x,y)) = (x,a')*(y,b') = \varphi((x,a))*\varphi((y,b)),$$

proving $\varphi \in \mathrm{Aut}(Q_{\mu\theta})$. □

5. A class of commutative A-loops of order p^3

Let Q be a commutative A-loop of odd order. Equivalently, let Q be a finite commutative A-loop in which the mapping $x \mapsto x^2$ is a bijection of Q (cf. [6, Lemma 3.1]). For $x \in Q$, denote by $x^{1/2}$ the unique element of Q such that $(x^{1/2})^2 = x$. Define a new operation $\circ$ on Q by

$$x \circ y = (x^{-1}\setminus xy^2)^{1/2}.$$

By [6, Lemma 3.5], $(Q,\circ)$ is a Bruck loop. By [6, Corollary 3.11], $(Q,\circ)$ is commutative if and only if it is isomorphic to Q.

Proposition 5.1. *Let p be an odd prime, and let Q be a commutative A-loop of order p, $2p$, $4p$, p^2, $2p^2$ or $4p^2$. Then Q is an abelian group.*

Proof. Loops of order less than 5 are abelian groups. By the Decomposition Theorem mentioned in the introduction, it remains to prove that commutative A-loops of order p and p^2 are abelian groups. For $|Q| = p$, this follows from the Lagrange Theorem and power-associativity. Assume that $|Q| = p^2$. Then $(Q,\circ)$ is a Bruck loop of order p^2. Burn showed in [3] that all Bol loops of order p^2 are groups, and hence $(Q,\circ)$ is an abelian group. Consequently, Q is an abelian group. □

In this section we initiate the study of commutative A-loops of order p^3. We conjecture that the class of loops constructed below accounts for all such loops.

Lemma 5.2. *There is no commutative A-loop with center of prime index.*

Proof. For a contradiction, let Q be a commutative A-loop such that $|Q/Z(Q)| = p$ for some prime p. By the Lagrange Theorem and power-associativity, $Q/Z(Q)$ is the cyclic group of order p. Let $x \in Q \setminus Z(Q)$. Then $|xZ(Q)| = p$ and every element of Q can be written as $x^i z$, where $0 \leq i < p$ and $z \in Z(Q)$. With $0 \leq i, j, k < p$ and $z_1, z_2, z_3 \in Z(Q)$ we have

$$(x^i z_1 \cdot x^j z_2) \cdot x^k z_3 = (x^i x^j) x^k \cdot z_1 z_2 z_3 = x^i (x^j x^k) \cdot z_1 z_2 z_3 = x^i z_1 \cdot (x^j z_2 \cdot x^k z_3)$$

by power-associativity, so Q is an abelian group with center of prime index, a contradiction. □

Hence a nonassociative commutative A-loop of order p^3 has center of size 1 or p. (By the result announced in the introduction, we know that the center has size p if p is odd.)

Let $n \geq 1$. The *overflow indicator* is the function $(-,-)_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \{0, 1\}$ defined by

$$(x, y)_n = \begin{cases} 1, & \text{if } x + y \geq n, \\ 0, & \text{otherwise.} \end{cases}$$

Note that for $x, y \in \mathbb{Z}_n$ we have $x \oplus y = x + y - n(x, y)_n$, and thus

$$(x, y)_n = \frac{x + y - (x \oplus y)}{n}, \tag{5.1}$$

where we use $\oplus$ to denote the addition in $\mathbb{Z}_n$, and $+$ to denote the addition in $\mathbb{Z}$.

Lemma 5.3. *We have*

$$(x, y)_n + (x \oplus y, z)_n = (y, z)_n + (x, y \oplus z)_n \tag{5.2}$$

for every x, y, $z \in \mathbb{Z}_n$.

Proof. Using (5.1), the identity (5.2) can be rewritten as

$$x + y - (x \oplus y) + (x \oplus y) + z - (x \oplus y \oplus z) = y + z - (y \oplus z) + x + (y \oplus z) - (x \oplus y \oplus z),$$

which holds. □

From now on we write $+$ for the addition in $\mathbb{Z}_n$, too.

For $n \geq 1$ and $a, b \in \mathbb{Z}_n$, define $\mathcal{Q}_{a,b}(\mathbb{Z}_n)$ on $\mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n$ by

$$(x_1, x_2, x_3)(y_1, y_2, y_3) = (x_1 + y_1 + (x_2 + y_2) x_3 y_3 + a(x_2, y_2)_n + b(x_3, y_3)_n, x_2 + y_2, x_3 + y_3). \tag{5.3}$$

Then $\mathcal{Q}_{a,b}(\mathbb{Z}_n)$ can be seen as a central extension of $\mathbb{Z}_n$ by $\mathbb{Z}_n \times \mathbb{Z}_n$ via the loop cocycle $\theta((x_2, x_3), (y_2, y_3)) = (x_2 + y_2) x_3 y_3 + a(x_2, y_2)_n + b(x_3, y_3)_n$, and hence $\mathcal{Q}_{a,b}(\mathbb{Z}_n)$ is a commutative loop with neutral element $(0, 0, 0)$.

Note that we can write θ as $\theta = \mu + \nu$, where $\mu((x_2, y_2), (x_3, y_3)) = (x_2 + y_2) x_3 y_3$ and $\nu((x_2, y_2), (x_3, y_3)) = a(x_2, y_2)_n + b(x_3, y_3)_n$. By Lemma 5.3, ν is a group cocycle.

Proposition 5.4. *Let $n \geq 2$ and $a, b \in \mathbb{Z}_n$. Let $Q = \mathcal{Q}_{a,b}(\mathbb{Z}_n)$ and $x = (x_1, x_2, x_3)$, $y = (y_1, y_2, y_3)$, $z = (z_1, z_2, z_3) \in Q$. Then:*

(i) $x \setminus y = (y_1 - x_1 - (y_3 - x_3) x_3 y_2 - a(x_2, y_2 - x_2)_n - b(x_3, y_3 - x_3)_n, y_2 - x_2, y_3 - x_3)$,
(ii) $xy \setminus x(yz) = (z_1 + y_3(x_3 z_2 - x_2 z_3), z_2, z_3)$,
(iii) *Q is a nonassociative commutative A-loop of order n^3,*
(iv) $N_\lambda(Q) = Z(Q) = \mathbb{Z}_n \times 0 \times 0$, $N_\mu(Q) = \mathbb{Z}_n \times \mathbb{Z}_n \times 0$ *as subsets of Q,*
(v) $Q/Z(Q) \cong \mathrm{Inn}(Q) \cong \mathbb{Z}_n \times \mathbb{Z}_n$, *and* $\mathrm{Inn}(Q) = \{L_{u,v};\ u, v \in Q\}$,
(vi) *for every $m \geq 0$, $x^m = (mx_1 + 2\binom{m+1}{3} x_2 x_3^2 + a t_2 + b t_3, m x_2, m x_3)$, where $t_i = \sum_{k=1}^{m-1} (x_i, k x_i)_n$. (As usual, the summation is considered empty and the binomial coefficient vanishes when $m < 2$.)*

Proof. Part (i) follows from the multiplication formula (5.3). Let $Q_0 = \mathcal{Q}_{0,0}(\mathbb{Z}_n)$. By Lemma 4.11, it suffices to verify the formula (ii) for Q_0 instead of for Q. Now, calculating in Q_0,

$$x(yz) = (x_1 + y_1 + z_1 + (y_2 + z_2)y_3z_3 + (x_2 + y_2 + z_2)x_3(y_3 + z_3), x_2 + y_2 + z_2, x_3 + y_3 + z_3),$$

so (i) for Q_0 implies that $xy \setminus x(yz)$ is equal to

$$(z_1 + (y_2 + z_2)y_3z_3 + (x_2 + y_2 + z_2)x_3(y_3 + z_3) - (x_2 + y_2)x_3y_3 - z_3(x_3 + y_3)(x_2 + y_2 + z_2), z_2, z_3),$$

which simplifies in a straightforward way to (ii).

By Lemma 4.12, to verify that left inner mappings of Q are automorphisms of Q, it suffices to check that the left inner mappings of Q_0 are automorphisms of Q_0. With $u = (u_1, u_2, u_3)$, $v = (v_1, v_2, v_3)$, use (ii) to see that

$$\begin{aligned}
&xy \setminus x(yu) \cdot xy \setminus x(yv)\\
&= (u_1 + y_3(x_3u_2 - x_2u_3), u_2, u_3)(v_1 + y_3(x_3v_2 - x_2v_3), v_2, v_3)\\
&= (u_1+v_1+y_3(x_3(u_2+v_2)-x_2(u_3, v_3))+(u_2+v_2)u_3v_3+a(u_2, v_2)_n+b(u_3, v_3)_n, u_2+v_2, u_3+v_3)\\
&= xy \setminus x(y \cdot uv).
\end{aligned}$$

Hence Q is a commutative A-loop of order n^3.

To calculate the middle nucleus, we can once again resort to the loop Q_0, since the group cocycle will not play any role in identities that follow from associativity. We have

$$\begin{aligned}
y \cdot (x_1, x_2, 0)z &= y(x_1 + z_1, x_2 + z_2, z_3)\\
&= (x_1 + y_1 + z_1 + (x_2 + y_2 + z_2)y_3z_3, x_2 + y_2 + z_2, y_3 + z_3)\\
&= (x_1 + y_1, x_2 + y_2, y_3)z = y(x_1, x_2, 0) \cdot z,
\end{aligned}$$

so $\mathbb{Z}_n \times \mathbb{Z}_n \times 0 \leq N_\mu(Q_0)$. On the other hand,

$$(0, 0, x_3)(x_1, x_2, 0) = (x_1, x_2, x_3),$$

so to prove that $(x_1, x_2, x_3) \notin N_\mu(Q_0)$ whenever $x_3 \neq 0$, it suffice so show that $(0, 0, x_3) \neq N_\mu(Q_0)$ whenever $x_3 \neq 0$. Now,

$$\begin{aligned}
(0, 0, 1) \cdot (0, 0, x_3)(0, 1, 0) &= (0, 0, 1)(0, 1, x_3) = (x_3, 1, 1 + x_3)\\
&\neq (0, 1, 1 + x_3) = (0, 0, 1 + x_3)(0, 1, 0) = (0, 0, 1)(0, 0, x_3) \cdot (0, 1, 0)
\end{aligned}$$

shows just that. Similarly,

$$\begin{aligned}
(x_1, 0, 0) \cdot yz &= (x_1, 0, 0)(y_1 + z_1 + (y_2 + z_2)y_3z_3, y_2 + z_2, y_3 + z_3)\\
&= (x_1 + y_1 + z_1 + (y_2 + z_2)y_3z_3, y_2 + z_2, y_3 + z_3)\\
&= (x_1 + y_1, y_2, y_3)z = (x_1, 0, 0)y \cdot z
\end{aligned}$$

proves that $\mathbb{Z}_n \times 0 \times 0 \leq N_\lambda(Q_0)$, and, for $x_2 \neq 0$,

$$\begin{aligned}
(x_1, x_2, 0) \cdot (0, 0, 1)(0, 0, 1) &= (x_1, x_2, 0)(0, 0, 2) = (x_1, x_2, 2)\\
&\neq (x_1 + x_2, x_2, 2) = (x_1, x_2, 1)(0, 0, 1) = (x_1, x_2, 0)(0, 0, 1) \cdot (0, 0, 1)
\end{aligned}$$

implies that $N_\lambda(Q) = \mathbb{Z}_n \times 0 \times 0$ (recall that $N_\lambda(Q) \leq N_\mu(Q)$ in any A-loop Q).

Consider the mapping $\varphi : Q \to \mathrm{Inn}(Q)$ defined by

$$\varphi(x_1, x_2, x_3) = L_{(0,x_2,x_3),(0,0,1)}.$$

Then

$$\begin{aligned}&\varphi(x_1,x_2,x_3)\varphi(y_1,y_2,y_3)(z_1,z_2,z_3)\\&=\varphi(x_1,x_2,x_3)(z_1+(y_3z_2-y_2z_3),z_2,z_3)=(z_1+y_3z_2-y_2z_3+(x_3z_2-x_2z_3),z_2,z_3)\\&=\varphi((x_1,x_2,x_3)(y_1,y_2,y_3))(z_1,z_2,z_3)\end{aligned}$$

and φ is a homomorphism. Its kernel consists of all $(x_1,x_2,x_3)\in Q$ such that $x_3z_2-x_2z_3=0$ for every $z_2,\ z_3\in Q$. Thus $\ker\varphi=\{(x_1,0,0);\ x_1\in\mathbb{Z}_n\}$. To prove (v), it remains to show that φ is onto $\mathrm{Inn}(Q)$. By (ii),

$$L_{(x_1,x_2,x_3),(y_1,y_2,y_3)}=L_{(0,x_2,x_3),(0,0,y_3)}=L_{(0,y_3x_2,y_3x_3),(0,0,1)}.$$

This means that $\mathrm{Im}\,\varphi$ contains a generating subset of $\mathrm{Inn}(Q)$, and hence it is equal to $\mathrm{Inn}(Q)$. In fact, purely of the grounds of cardinality, we have $\mathrm{Inn}(Q)=\{L_{u,v};\ u,\ v\in Q\}$.

The identity of (vi) clearly holds when $m=0$. Assume that it holds for some $m\geq 0$. Let $t_i^m=\sum_{k=1}^m(x_i,kx_i)_n$. By power-associativity, we have

$$\begin{aligned}x^{m+1}=xx^m&=x(mx_1+2\binom{m+1}{3}x_2x_3^2+at_2^{m-1}+bt_3^{m-1},mx_2,mx_3)\\&=((m+1)x_1+2\binom{m+1}{3}x_2x_3^2+(m+1)x_2mx_3^2+at_2^m+bt_3^m,(m+1)x_2,(m+1)x_3),\end{aligned}$$

Since $2\binom{m+1}{3}+(m+1)m=2\binom{m+2}{3}$, we are through. □

Lemma 5.5. *Let p be a prime and $a,\ b\in\mathbb{Z}_p$. Let $Q=\mathcal{Q}_{a,b}(\mathbb{Z}_p)$. Then:*

(i) *if $(a,b)=(0,0)$ and $p\neq 3$ then Q has exponent p,*
(ii) *if $(a,b)\neq(0,0)$ or $p=3$ then Q has exponent p^2,*
(iii) *if $a=0$ then $N_\mu(Q)\cong\mathbb{Z}_p\times\mathbb{Z}_p$,*
(iv) *if $a\neq 0$ then $N_\mu(Q)\cong\mathbb{Z}_{p^2}$.*

Proof. By [6], every element of Q has order a power of p, so Q has exponent p, p^2 or p^3. Since Q is nonassociative by Proposition 5.4, the exponent is either p or p^2.

Assume that $(a,b)=(0,0)$. Then by Proposition 5.4(vi),

$$(x_1,x_2,x_3)^p=(2\binom{p+1}{3}x_2x_3^2,0,0).$$

The integer $2\binom{p+1}{3}$ is divisible by p if and only if $p\neq 3$. This proves (i).

To show (ii), it remains to prove that Q has exponent p^2 if $(a,b)\neq(0,0)$. Assume that $a\neq 0$, and note that, by Proposition 5.4(vi),

$$(0,1,0)^p=(a\sum_{k=1}^{p-1}(1,k)_p,0,0)=(a(1,p-1)_p,0,0)=(a,0,0).$$

This means that Q does not have exponent p, and it also shows, by Proposition 5.4(iv), that $N_\mu(Q)\cong\mathbb{Z}_{p^2}$. Similarly, when $b\neq 0$, use

$$(0,0,1)^p=(b\sum_{k=1}^{p-1}(1,k)_p,0,0)=(b,0,0)$$

to conclude that Q does not have exponent p.

Finally, when $a=0$, we have $(x_1,x_2,0)^p=0$ by Proposition 5.4(vi), so $N_\mu(Q)\cong\mathbb{Z}_p\times\mathbb{Z}_p$ by Proposition 5.4(iv). □

Lemma 5.6. *Let $n>0$. If $b,\ c\in\mathbb{Z}_n^*$ then $\mathcal{Q}_{0,b}(\mathbb{Z}_n)\cong\mathcal{Q}_{0,c}(\mathbb{Z}_n)$.*

Proof. Define $\varphi : \mathcal{Q}_{0,b}(\mathbb{Z}_n) \to \mathcal{Q}_{0,c}(\mathbb{Z}_n)$ by $(x_1, x_2, x_3) \mapsto ((c/b)x_1, (c/b)x_2, x_3)$, and note that φ is a bijection since b, c are invertible.

Denote by $\cdot$ the multiplication in $\mathcal{Q}_{0,b}(\mathbb{Z}_n)$ and by $*$ the multiplication in $\mathcal{Q}_{0,c}(\mathbb{Z}_n)$. Then

$$\begin{aligned}\varphi((x_1, x_2, x_3) \cdot (y_1, y_2, y_3)) &= \varphi((x_1 + y_1 + (x_2 + y_2)x_3y_3 + b(x_3, y_3)_n, x_2 + y_2, x_3 + y_3))\\ &= (\frac{c}{b}(x_1 + y_1 + (x_2 + y_2)x_3y_3 + b(x_3, y_3)_n), \frac{c}{b}(x_2 + y_2), x_3 + y_3)\\ &= (\frac{c}{b}x_1, \frac{c}{b}x_2, x_3) * (\frac{c}{b}y_1, \frac{c}{b}y_2, y_3) = \varphi((x_1, x_2, x_3)) * \varphi((y_1, y_2, y_3)).\end{aligned}$$

□

Let p be an odd prime. Recall that $a \in \mathbb{Z}_p^*$ is a *quadratic residue modulo p* if there is $x \in \mathbb{Z}_p^*$ such that $x^2 \equiv a \pmod p$. Else a is a *quadratic nonresidue modulo p*. The well-known Legendre symbol identity $(ab/p) = (a/p)(b/p)$ shows that ab^{-1} is a quadratic residue if and only if either both a, b are quadratic residues or both a, b are quadratic nonresidues.

Lemma 5.7. *Let p be an odd prime and a_1, $a_2 \in \mathbb{Z}_p^*$. If a_1, a_2 are either both quadratic residues or both quadratic nonresidues then $\mathcal{Q}_{a_1,0}(\mathbb{Z}_p) \cong \mathcal{Q}_{a_2,0}(\mathbb{Z}_p)$.*

Proof. Since $a_1a_2^{-1}$ is a quadratic residue, there is u such that $a_2 = a_1u^2$. Define $\varphi : \mathcal{Q}_{a_1,0}(\mathbb{Z}_p) \to \mathcal{Q}_{a_2,0}(\mathbb{Z}_p)$ by $(x_1, x_2, x_3) \mapsto (u^2x_1, x_2, ux_3)$. Then φ is a bijection. Denote by $\cdot$ the multiplication in $\mathcal{Q}_{a_1,0}(\mathbb{Z}_p)$ and by $*$ the multiplication in $\mathcal{Q}_{a_2,0}(\mathbb{Z}_p)$. Then

$$\begin{aligned}\varphi((x_1, x_2, x_3) \cdot (y_1, y_2, y_3)) &= \varphi((x_1 + y_1 + (x_2 + y_2)x_3y_3 + a_1(x_2, y_2)_p, x_2 + y_2, x_3 + y_3))\\ &= (u^2(x_1 + y_1 + (x_2 + y_2)x_3y_3 + a_1(x_2, y_2)_p), x_2 + y_2, u(x_3 + y_3))\\ &= (u^2x_1 + u^2y_1 + (x_2 + y_2)ux_3uy_3 + a_2(x_2, y_2)_p, x_2 + y_2, u(x_3 + y_3))\\ &= (u^2x_1, x_2, ux_3) * (u^2y_1, y_2, uy_3) = \varphi((x_1, x_2, x_3)) * \varphi((y_1, y_2, y_3)).\end{aligned}$$

□

Lemma 5.8. *For a prime p, let $Q_1 = \mathcal{Q}_{a,b}(\mathbb{Z}_p)$, $Q_2 = \mathcal{Q}_{a,c}(\mathbb{Z}_p)$ and let $f : Q_1 \to Q_2$ be an isomorphism that pointwise fixes the middle nucleus of Q_1 (i.e., f is identical on $\mathbb{Z}_p \times \mathbb{Z}_p \times 0$). Then there are A, $B \in \mathbb{Z}_p$ and $C \in \mathbb{Z}_p^*$ such that*

$$f(x_1, x_2, x_3) = (x_1, x_2, 0) * (A, B, C)^{x_3} \tag{5.4}$$

for every $(x_1, x_2, x_3) \in Q_1$.

In addition, every mapping $f : Q_1 \to Q_2$ defined by (5.4) with A, $B \in \mathbb{Z}_p$ and $C \in \mathbb{Z}_p^*$ is a bijection that pointwise fixes $N_\mu(Q_1)$.

Proof. Let $f : Q_1 \to Q_2$ be an isomorphism that pointwise fixes $N_\mu(Q_1)$. As $Q_1/N_\mu(Q_1)$ is a cyclic group, f is determined by the image of any element in $Q_1 \setminus N_\mu(Q_1)$. Let $f(0, 0, 1) = (A, B, C)$. We must have $C \neq 0$, else f is not a bijection. Since $(x_1, x_2, x_3) = (x_1, x_2, 0)(0, 0, x_3)$ and $(0, 0, x_3) = (0, 0, 1)^{x_3}$ by Proposition 5.4(vi), we have

$$f(x_1, x_2, x_3) = f(x_1, x_2, 0) * f(0, 0, 1)^{x_3} = (x_1, x_2, 0) * (A, B, C)^{x_3}.$$

Conversely, define $f : Q_1 \to Q_2$ by (5.4), where $C \neq 0$. Then f obviously pointwise fixes $N_\mu(Q_1)$. To show that f is a bijection, assume that $f(x_1, x_2, x_3) = f(y_1, y_2, y_3)$. Since the last coordinate of $(x_1, x_2, 0) * (A, B, C)^{x_3}$ is Cx_3, we conclude that $x_3 = y_3$. The second coordinate of $(x_1, x_2, 0) * (A, B, C)^{x_3}$ is $x_2 + Bx_3$, and we conclude that $x_2 = y_2$. Then $x_1 = y_1$ follows from the multiplication formula for Q_2 and from Proposition 5.4(vi). □

Lemma 5.9. *Let $p \neq 3$ be a prime and assume that a, b, $c \in \mathbb{Z}_p$ are such that $a + c \equiv b \pmod p$. Let $Q_1 = \mathcal{Q}_{a,b}(\mathbb{Z}_p) = (Q_1, \cdot)$ and $Q_2 = \mathcal{Q}_{a,c}(\mathbb{Z}_p) = (Q_2, *)$. Then $f : Q_1 \to Q_2$ defined by (5.4) with $(A, B, C) = (0, 1, 1)$ is an isomorphism.*

Proof. For $x \in \mathbb{Z}_p$, let $x' = (x-1)x(x+1)/3$. By Lemma 5.8, f is a bijection onto Q_2 that pointwise fixes $N_\mu(Q_1)$. Upon expanding the formula (5.4), we see that

$$f(x_1, x_2, x_3) = (x_1 + x_3' + a(x_2, x_3)_p, x_2 + x_3, x_3),$$

since the expression $\sum_{k=1}^{x_3-1}(1,k)_p$ vanishes for every x_3. Let $(u_1, u_2, u_3) = f(x_1, x_2, x_3) * f(y_1, y_2, y_3)$ and $(v_1, v_2, v_3) = f((x_1, x_2, x_3) \cdot (y_1, y_2, y_3))$. A quick calculation then shows that

$$(u_2, u_3) = (v_2, v_3) = (x_2 + x_3 + y_2 + y_3, x_3 + y_3),$$

u_1 is equal to

$$x_1+x_3'+a(x_2,x_3)_p+y_1+y_3'+a(y_2,y_3)_p+(x_2+x_3+y_2+y_3)x_3y_3+a(x_2+x_3,y_2+y_3)_p+c(x_3,y_3)_p,$$

while v_1 is equal to

$$x_1+y_1+(x_2+y_2)x_3y_3+a(x_2,y_2)_p+b(x_3,y_3)_p+(x_3+y_3)'+a(x_2+y_2,x_3+y_3)_p.$$

Now, $x_3' + y_3' = (x_2 + y_2)x_3y_3 + (x_3 + y_3)'$. Using (5.1), it is easy to see that

$$(x_2, x_3)_p + (y_2, y_3)_p + (x_2 + x_3, y_2 + y_3)_p = (x_2, y_2)_p + (x_2 + y_2, x_3 + y_3)_p + (x_3, y_3)_p.$$

Hence we are done by $a + c \equiv b \pmod p$. □

Corollary 5.10. *Let $p \neq 3$ be a prime, $a \in \mathbb{Z}_p^*$ and b, $c \in \mathbb{Z}_p$. Then $\mathcal{Q}_{a,b}(\mathbb{Z}_p)$ is isomorphic to $\mathcal{Q}_{a,c}(\mathbb{Z}_p)$.*

Proof. By Lemma 5.9 we have $\mathcal{Q}_{a,0}(\mathbb{Z}_p) \cong \mathcal{Q}_{a,a}(\mathbb{Z}_p) \cong \mathcal{Q}_{a,2a}(\mathbb{Z}_p)$, and so on. □

5.1. **Ring construction.** Note that for $a = b = 0$, the construction (5.3) makes sense over any commutative ring R, not just over $\mathbb{Z}_n$. We can summarize the most important features of the construction as follows:

Proposition 5.11. *Let $R \neq 0$ be a commutative ring. Let $Q = \mathcal{Q}(R)$ be defined on $R \times R \times R$ by*

$$(x_1, x_2, x_3)(y_1, y_2, y_3) = (x_1 + y_1 + (y_2 + x_2)x_3y_3, x_2 + y_2, x_3 + y_3).$$

Then Q is a commutative A-loop satisfying $N_\lambda(Q) = Z(Q) = R\times 0\times 0$ and $N_\mu(Q) = R\times R\times 0$.

Proof. See the relevant parts of the proof of Proposition 5.4. □

5.2. **Towards the classification of commutative A-loops of order p^3.** The results obtained up to this point come close to describing the isomorphism types of all loops $\mathcal{Q}_{a,b}(\mathbb{Z}_p)$ for all primes $p \neq 3$.

Fix $p \neq 3$. The loop $\mathcal{Q}_{0,0}(\mathbb{Z}_p)$ is of exponent p and is not isomorphic to any other loop $\mathcal{Q}_{a,b}(\mathbb{Z}_p)$, by Lemma 5.5. By Lemmas 5.5 and 5.6, the loops $\{\mathcal{Q}_{0,b}(\mathbb{Z}_p);\ 0 < b < p\}$ form an isomorphism class. By Lemmas 5.7 and 5.8, each of the two sets $I_r = \{\mathcal{Q}_{a,b}(\mathbb{Z}_p);\ a > 0$ is a quadratic residue modulo p and $0 \leq b \leq p-1\}$ and $I_n = \{\mathcal{Q}_{a,b}(\mathbb{Z}_p);\ a > 0$ is a quadratic nonresidue modulo p and $0 \leq b \leq p-1\}$ consist of pairwise isomorphic loops.

However, we did not manage to establish the following:

Conjecture 5.12. *Let $p > 3$ be a prime, let $a_1 \in \mathbb{Z}_p^*$ be a quadratic residue and $a_2 \in \mathbb{Z}_p^*$ be a quadratic nonresidue. Then $\mathcal{Q}_{a_1,0}(\mathbb{Z}_p)$ is not isomorphic to $\mathcal{Q}_{a_2,0}(\mathbb{Z}_p)$.*

We have verified the conjecture computationally with the GAP [5] package LOOPS [8] for $p = 5, 7$. It appears that one of the distinguishing isomorphism invariants is the multiplication group $\mathrm{Mlt}(Q) = \langle L_x, R_x;\ x \in Q\rangle$.

The loops $\mathcal{Q}_{a,b}(\mathbb{Z}_p)$ behave differently for $p = 3$ due to the fact that 3 is the only prime p for which p does not divide $2\binom{p+1}{3}$. Denote by $f_{(A,B,C)}$ the bijection defined by (5.4). It can be verified by computer that $f_{(0,1,1)}$ is an exceptional isomorphism $\mathcal{Q}_{0,0}(\mathbb{Z}_3) \to \mathcal{Q}_{0,1}(\mathbb{Z}_3)$, $f_{(0,0,2)}$

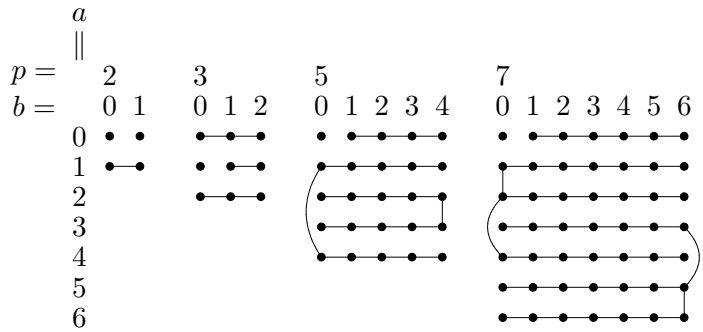

FIGURE 1. Isomorphism classes of loops $\mathcal{Q}_{a,b}(\mathbb{Z}_p)$ for $p \in \{2, 3, 5, 7\}$.

is an isomorphism $\mathcal{Q}_{1,1}(\mathbb{Z}_3) \to \mathcal{Q}_{1,2}(\mathbb{Z}_3)$, $f_{(0,1,2)}$ is an isomorphism $\mathcal{Q}_{2,0}(\mathbb{Z}_3) \to \mathcal{Q}_{2,1}(\mathbb{Z}_3)$ and $f_{(0,1,1)}$ is an isomorphism $\mathcal{Q}_{2,0}(\mathbb{Z}_3) \to \mathcal{Q}_{2,2}(\mathbb{Z}_3)$. The loops $\mathcal{Q}_{0,0}(\mathbb{Z}_3)$, $\mathcal{Q}_{1,0}(\mathbb{Z}_3)$, $\mathcal{Q}_{1,1}(\mathbb{Z}_3)$ and $\mathcal{Q}_{2,0}(\mathbb{Z}_3)$ contain precisely 12, 6, 24 and 18 elements of order 9, respectively, so no two of them are isomorphic.

Altogether, Figure 1 depicts the isomorphism classes of loops $\mathcal{Q}_{a,b}(\mathbb{Z}_p)$ as connected components, for $p \in \{2, 3, 5, 7\}$ and a, $b \in \mathbb{Z}_p$. Moreover, if Conjecture 5.12 is true, the pattern established by $p = 2$, 5 and 7 continues for all primes $p > 7$.

It is reasonable to ask whether, for an odd prime p, there are nonassociative commutative A-loops of order p^3 not of the form $\mathcal{Q}_{a,b}(\mathbb{Z}_p)$.

Using a linear-algebraic approach to cocycles (see Subsection 6.4), we managed to classify all nonassociative commutative A-loops of order p^3 with nontrivial center, for $p \in \{2, 3, 5, 7\}$. It turns out that all such loops are of the type $\mathcal{Q}_{a,b}(\mathbb{Z}_p)$. In particular, $p = 3$ is the only prime for which there is no nonassociative commutative A-loop of order p^3 and exponent p.

Problem 5.13. *Let p be an odd prime and Q a nonassociative commutative A-loop of order p^3. Is Q isomorphic to $\mathcal{Q}_{a,b}(\mathbb{Z}_p)$ for some a, $b \in \mathbb{Z}_p$?*

6. Enumeration

We believe that future work will benefit from an enumeration of small commutative A-loops. The results are summarized in Table 1, which lists all orders $n \leq 32$ for which there exists a nonassociative commutative A-loop.

In the table, $Z(Q)$ refers to the center of Q, and $A(Q)$ refers to the *associator subloop* of Q, that is, the smallest normal subloop of Q such that $Q/A(Q)$ is a group. For instance, the row labeled by $A(Q) \neq 1$, $Z(Q) \neq 1$ counts all nonassociative commutative A-loops with nontrivial center, and the row labeled by $A(Q) \neq 1$, $Q^p = 1$ counts all nonassociative commutative A-loops of exponent p (for the appropriate prime p).

In the table, if there is only one number in a cell, it is both the number of isomorphism classes and the number of isotopism classes. If there are two numbers in a cell, the first one is the number of isomorphism classes and the second one (in parentheses) is the number of isotopism classes.

All computations were done with the finite model builder Mace4 and with the GAP package LOOPS on a Unix machine with a single 2 GHz processor, with computational times for individual orders ranging from seconds to hours.

TABLE 1. Commutative A-loops up to isomorphism and up to isotopism.

n	8	15	16	21	24	27	30	32
$A(Q)=1$	3	1	5	1	3	3	1	7
$A(Q)\neq 1$	4(3)	1	46(38)	1	4(3)	4	1	?
$A(Q)\neq 1$ $Z(Q)\neq 1$	3(2)	0	44(37)	0	4(3)	4	1	?
$A(Q)\neq 1$ $Q^p=1$	2	–	12(11)	–	–	0	–	?
$A(Q)\neq 1$ $Z(Q)\neq 1$ $Q^p=1$	1	–	10	–	–	0	–	211(210)

6.1. **Comments on commutative A-loops of order** 8**.** For classification up to isomorphism, see Section 3.

Lemma 6.1. *Let G be a commutative loop, $g\in \mathrm{Aut}(G)$, and let t_1, t_2 be fixed points of g. Define $f_i(x)=g(x)t_i$, for $i=1$, 2. If there is $z\in G$ such that $g(z)=z^{-1}t_1^{-1}t_2$, then $G(f_1)$, $G(f_2)$ are isotopic.*

Proof. Denote by $*$ the multiplication in $G(f_1)$ and by $\circ$ the multiplication in $G(f_2)$. For $x\in G$, define $\alpha(x)=x$, $\alpha(\overline{x})=\overline{xr^{-1}}$, $\beta(x)=rx$, $\beta(\overline{x})=\overline{x}$, $\gamma(x)=rx$, and $\gamma(\overline{x})=\overline{x}$. Then

$$\begin{aligned}
&\alpha(x)\circ\beta(y)=x\circ ry=xry=\gamma(xy)=\gamma(x*y),\\
&\alpha(x)\circ\beta(\overline{y})=x\circ\overline{y}=\overline{xy}=\gamma(\overline{xy})=\gamma(x*\overline{y}),\\
&\alpha(\overline{x})\circ\beta(y)=\overline{xr^{-1}}\circ ry=\overline{xy}=\gamma(\overline{xy})=\gamma(\overline{x}*y),\\
&\alpha(\overline{x})\circ\beta(\overline{y})=\overline{xz^{-1}}\circ\overline{y}=g(xz^{-1}y)t_2=zg(xy)t_1=\gamma(g(xy)t_1)=\gamma(\overline{x}*\overline{y}),
\end{aligned}$$

where we have used $g(z)=z^{-1}t_1^{-1}t_2$ in the last line. □

Let $G=\mathbb{Z}_2\times\mathbb{Z}_2=\langle a\rangle\times\langle b\rangle$ be the Klein group. Consider the transposition $g=(a,b)$ with fixed points $t_1=1$, $t_2=ab$. Let $f_i(x)=g(x)t_i$, for $i=1$, 2. Then $b=g(a)=a^{-1}t_1^{-1}t_2$, so $G(f_1)$, $G(f_2)$ are isotopic by Lemma 6.1.

6.2. **Comments on commutative A-loops of order** 15 **and** 21**.**

Lemma 6.2. *Let Q be a nonassociative commutative A-loop of order p_0p_1, where $p_0\neq p_1$ are odd primes. Then there is $0\leq i\leq 1$ such that Q contains a normal subloop S of order p_i, and all elements in $Q\setminus S$ have order p_{i+1}, where the subscript is calculated modulo* 2*.*

Proof. We will use results of [6] mentioned in the introduction without further reference. Since Q is of odd order, it is solvable. Since Q is also nonassociative, there is a normal subloop S of Q such that $1\neq S\neq Q$. By the Lagrange Theorem, $|S|=p_i$ for some $0\leq i\leq 1$. Without loss of generality, let $|S|=p_0$. Let $y\in Q\setminus S$ and let T be the preimage of the subloop $\langle yS\rangle$ of Q/S. By the Lagrange Theorem again, $y^{p_1}=1$, as the only other alternative $|y|=p_0p_1$ would mean that Q is a group by power-associativity. □

The information afforded by Lemma 6.2 is sufficient to construct all nonassociative commutative A-loops of order 15 and 21 by the finite model builder Mace4. It turns out that in each case there is a unique such loop. These two loops were constructed already by Drápal [4, Proposition 3.1]. Nevertheless the following problem remains open:

Problem 6.3. *Classify commutative A-loops of order pq, where $p < q$ are odd primes.*

We have some reasons to believe that there is no nonassociative commutative A-loop of order 35.

6.3. **Comments on commutative A-loops of order** 16**.** Among the 12 nonassociative commutative A-loops of order 16 and exponent 2, three have inner mapping groups of orders that are not a power of 2, namely 12, 56 and 56. We now construct the two nonassociative commutative A-loops of order 16 and exponent 2 with inner mapping groups of order 56, and we show that they are isotopic.

Let $G = \mathbb{Z}_4 \times \mathbb{Z}_2$. Define $g \in \mathrm{Aut}(G)$ by $g(i, j) = (i, i + j \mod 2)$. Note that $t_1 = (0, 0)$, $t_2 = (2, 1)$ are fixed points of g, and let $f_i(x) = g(x) + t_i$. Then $G(f_1)$, $G(f_2)$ are the two announced loops, and they are isotopic by Lemma 6.1, since $g(1, 0) = (1, 1)$ and $-(1, 0) - (0, 0) + (2, 1) = (1, 1)$.

6.4. **Comments on commutative A-loops of order** 32 **and exponent** 2 **with nontrivial center.** The methods developed in [9] in order to classify Moufang loops of order 64 can be adopted to other classes of loops. Using the cocycle formula of Corollary 4.1 and the classification of commutative A-loops of order 16 from Subsection 6.3, we were able to classify all commutative A-loops of order 32 and of exponent 2 with nontrivial center.

We now briefly describe the search, following the method of [9] closely. For more details, see [9].

Let Q be a commutative A-loop of order 32 and exponent 2 with nontrivial center. Then $Z(Q)$ is obviously an elementary abelian 2-group, and hence it possesses a 2-element central subgroup $Z = (Z, +, 0)$. Then $Q/Z = K$ is a commutative A-loop of order 16 and exponent 2.

The loop cocycles $\theta : K \times K \to Z$ form a vector space V over $Z = \mathrm{GF}(2)$ with respect to addition $(\theta + \mu)(x, y) = \theta(x, y) + \mu(x, y)$. The vector space V has basis $\{\theta_{u,v};\ 1 \neq u \in K,\ 1 \neq v \in K\}$, where

$$\theta_{u,v}(x, y) = \begin{cases} 1, & \text{if } (u, v) = (x, y), \\ 0, & \text{otherwise.} \end{cases}$$

The extension $K \ltimes_\theta Z$ will be a commutative A-loop of exponent 2 if and only if θ belongs to the subspace $C = \{\theta \in V;\ \theta \text{ satisfies (4.1)}, \theta(x, x) = 0 \text{ for every } x \in K \text{ and } \theta(x, y) = \theta(y, x) \text{ for every } x, y \in K\}$.

For every x, y, z, $x' \in K$, the equation (4.1) can be viewed as a linear equation over $\mathrm{GF}(2)$ in variables $\theta_{u,v}$. Similarly, for every x, $y \in K$ we obtain linear equations from the condition $\theta(x, y) = \theta(y, x)$, and from $\theta(x, x) = 0$.

Upon solving this system of linear equations, we obtain (a basis of) C, and it is in principle possible to construct all extensions $K \ltimes_\theta Z$ for $\theta \in C$. The two computational problems we face are: (i) the dimension of C can be large, (ii) it is costly to sort the resulting loops up to isomorphism. In order to overcome these obstacles, we take advantage of coboundaries and of an induced action of $\mathrm{Aut}(K)$ on C.

Let $\tau : K \times Z$ be a mapping satisfying $\tau(1) = 0$. Then $\delta\tau : K \times K \to Z$ defined by

$$\delta\tau(x, y) = \tau(xy) - \tau(x) - \tau(y)$$

is a *coboundary*. Coboundaries form a subspace B of V.

In fact, B is a subspace of C. This can be proved explicitly by verifying that every coboundary $\theta = \delta\tau$ satisfies the identity (4.1), $\theta(x, y) = \theta(y, x)$ and $\theta(x, x) = 0$. The verification of (4.1) is a bit unpleasant, so it is worth realizing that every coboundary θ satisfies the group cocycle identity

$$\theta(x, y) + \theta(xy, z) = \theta(y, x) + \theta(x, yz),$$

and hence also any cocycle identity that follows from associativity, in particular (4.1).

Moreover, if θ, $\mu : K \times K \to Z$ are two cocycles such that $\theta - \mu$ is a coboundary, then $K \ltimes_\theta Z$ is isomorphic to $K \ltimes_\theta Z$, cf. [9, Lemma 9]. It therefore suffices to construct loops $K \ltimes_\theta Z$, where $\theta \in D$, $C = B \oplus D$.

Given $\theta \in V$ and $\varphi \in \mathrm{Aut}(K)$, we define $\theta_\varphi \in V$ by

$$\theta_\varphi(x, y) = \theta(\varphi(x), \varphi(y)).$$

This action of $\mathrm{Aut}(K)$ on V induces an action on D. Moreover, by [9, Lemma 14], $K \ltimes_\theta Z$ is isomorphic to $K \ltimes_{\theta_\varphi} Z$. It therefore suffices to construct loops $K \ltimes_\theta Z$, where we take one θ from each orbit of $\mathrm{Aut}(K)$ on D.

Using each of the 13 commutative A-loops of order 16 and exponent 2 as K (the elementary abelian group of order 16 must also be taken into account), the above search finds 355 commutative A-loops of order 32 and exponent 2 within several minutes. The final isomorphism search takes several hours.

The lone isotopism $\mathbb{Z}_2 \times Q_1 \to \mathbb{Z}_2 \times Q_2$ is induced by the isotopism $Q_1 \to Q_2$ described in Subsection 6.3.

References

[1] R. H. Bruck, A survey of binary systems, third printing, corrected, *Ergebnisse der Mathematik und Ihrer Grenzgebiete*, new series, volume **20**, Springer, 1971.

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

[3] R. P. Burn, *Finite Bol loops*, Math. Proc. Cambridge Philos. Soc. **84** (1978), no. **3**, 377–385.

[4] A. Drápal, *A class of commutative loops with metacyclic inner mapping groups*, submitted.

[5] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*; 2004, `http://www.gap-system.org`.

[6] P. Jedlička, M. K. Kinyon and P. Vojtěchovský, *The structure of commutative automorphic loops*, submitted.

[7] W. McCune, *Prover9* and *Mace4*, `http://www.prover9.org`.

[8] G. P. Nagy and P. Vojtěchovský, *LOOPS: Computing with quasigroups and loops*, version 2.0.0, package for GAP, `http://www.math.du.edu/loops`.

[9] G. P. Nagy and P. Vojtěchovský, *The Moufang loops of order* 64 *and* 81, J. Symbolic Computation **42** (2007), no. **9**, 871–883.

[10] H. O. Pflugfelder, Quasigroups and Loops: Introduction, *Sigma Series in Pure Mathematics* **7**, Heldermann Verlag Berlin, 1990.

(Jedlička) Department of Mathematics, Faculty of Engineering, Czech University of Life Sciences, Kamýcká 129, 165 21 Prague 6-Suchdol, Czech Republic

E-mail address, Jedlička: `jedlickap@tf.czu.cz`

(Kinyon) Department of Mathematics, University of Denver, 2360 S Gaylord St, Denver, Colorado, 80208, U.S.A.

E-mail address, Kinyon: `mkinyon@math.du.edu`

(Vojtěchovský) Department of Mathematics, University of Denver, 2360 S Gaylord St, Denver, Colorado, 80208, U.S.A.

E-mail address, Vojtěchovský: `petr@math.du.edu`