Charles University in Prague
Faculty of Mathematics and Physics

HABILITATION THESIS

Přemysl Jedlička

Commutative automorphic loops

Matematika – algebra, teorie čísel a matematická logika

Preface

This habilitation thesis presents selected papers on the topic of commutative automorphic loops. The first chapter is an introduction to the topic. The remaining chapters contain reprints of the following articles:

2. Přemysl Jedlička, Michael K. Kinyon, Petr Vojtěchovský:
   Constructions of commutative automorphic loops,
   Communications in Algebra **38**,9 (2010), 3243–3267

3. Přemysl Jedlička, Michael K. Kinyon, Petr Vojtěchovský:
   The structure of commutative automorphic loops,
   Transactions of American Mathematical Society **363**,1 (2011), 365–384

4. Přemysl Jedlička, Michael K. Kinyon, Petr Vojtěchovský:
   Nilpotency in automorphic loops of prime power order,
   Journal of Algebra **350** (2012), 64–76

5. Přemysl Jedlička, Denis Simon:
   On commutative A-loops of order pq,
   Journal of Algebra and its Applications **14**,3 (2014), 20 pages

6. Jan Hora, Přemysl Jedlička:
   Nuclear semidirect product of commutative automorphic loops,
   Journal of Algebra and its Applications **13**,1 (2014), 15 pages

7. Přemysl Jedlička:
   Odd order semidirect extensions of commutative automorphic loops,
   Commentationes Mathematicae Universitatis Carolinae **55**,4 (2014), 447–456

Contents

1 Introduction

Loop theory is a branch of abstract algebra sitting between group theory, universal algebra and combinatorics. Its main object—a loop—is, vaguely said, a group without associativity; more precisely it is an algebra Q with a single binary operation $\cdot$ satisfying

- for all x, y in Q there exists a unique z with $x \cdot z = y$; (left quasigroup)
- for all x, y in Q there exists a unique z with $z \cdot x = y$; (right quasigroup)
- there exists a (unique) element 1 in Q such that $x \cdot 1 = 1 \cdot x = x$, for all $x \in Q$. (neutral element)

From the combinatorial point of view, a loop is a latin square with the first row and the first column prescribed. From the universal algebraic point of view, it is useful to define companion operations / and \; a loop is then an algebra $(Q, \cdot, /, \backslash, 1)$ satisfying

$$\begin{aligned} &1 \cdot x = x, && (x \cdot y)/y = x, && (x/y) \cdot y = x, \\ &x \cdot 1 = x, && x\backslash(x \cdot y) = y, && x \cdot (x\backslash y) = y. \end{aligned}$$

These division operations have to be taken into account when constructing subloops and congruences.

Loops share some properties with groups, e.g. the work with congruences: in group theory we work with normal subgroups instead of congruences. The same principle applies for loops—given a homomorphism from a loop to a loop, all preimages of elements are copies of the preimage of 1 and this subset turns out to be a subloop called the kernel. And a subloop is called normal if it is a kernel of some homomorphism; we shall, later on, give another characterisation of normal subloops.

There are several other notions that can be naturally pulled from group theory into loop theory but most of group properties fail to hold in loops. Consider, for instance, one of the smallest non-associative loops:

	1	2	3	4	5
1	1	2	3	4	5
2	2	1	5	3	4
3	3	4	1	5	2
4	4	5	2	1	3
5	5	3	4	2	1

(1)

This is a loop of order 5 where every element has order 2. Hence we see that even Lagrange's property does not hold for loops in general (some orders of subloops do not divide the order of the loop), let alone that the order of an element itself needs not be defined in some loops.

1 Loops of Bol-Moufang type

In order to obtain stronger structural results, researchers usually focus on narrower classes of loops, usually such classes that contain all the groups. The most famous class of loops are Moufang loops, which satisfy one of the four following equivalent identities:

$$\begin{aligned} &x \cdot (y \cdot (x \cdot z)) = ((x \cdot y) \cdot x) \cdot z, && (x \cdot y) \cdot (z \cdot x) = (x \cdot (y \cdot z)) \cdot x, \\ &(x \cdot y) \cdot (z \cdot x) = x \cdot ((y \cdot z) \cdot x), && y \cdot ((x \cdot z) \cdot x) = ((y \cdot x) \cdot z) \cdot x. \end{aligned} \tag{2}$$

This class was first studied by Ruth Moufang on the example of octonions: the multiplication operation of octonions is not associative anymore but it turns out to satisfy (2). Other examples are code loops that are used to construct some error-correcting codes or Parker's loop that was used to construct the Monster group.

Moufang loops form the best-known class of loops. Nevertheless, some of the results needed lots of efforts, for instance, the Lagrange property for Moufang loops was proved as late as 2005, by A. Grishkov and A. Zavarnitsine [16] and independently by J. Hall and S. Gagola III [10]. Both the proofs needed the classification of simple groups which is itself a highly non-trivial result.

Another example of a famous loop class are so called Bol loops, defined by the identity

$$x \cdot (y \cdot (x \cdot z)) = (x \cdot (y \cdot x)) \cdot z.$$

Examples are, e.g., all Moufang loops. These loops are power-associative, that means, all mono-generated subloops are groups. Hence it makes sense to define x^k, for any integer k.

If Bol loops satisfy also

$$(x \cdot y)^{-1} = x^{-1}y^{-1},$$

then they are called Bruck loops or K-loops. They are found naturally in several settings, for instance in Einstein's relativity theory. Bruck loops play a prominent rôle in the loop theory because of the work of G. Glauberman [11]: suppose that $(Q, \cdot)$ is a Moufang loop such that the squaring $x \mapsto x^2$ is a bijection. Then $(Q, \circ)$ with $x \circ y = \sqrt{xy^2x}$ is a Bruck loop sharing many properties with the Moufang loop $(Q, \cdot)$. Hence many Moufang loop properties were first proved for Bruck loops and then pushed to the Moufang world.

2 Permutation groups on loops

In loops, a crucial structure is so called multiplication group, which is a permutation group acting on the loop. We define left and right translations as follows:

$$L_a : x \mapsto ax, \qquad R_a : x \mapsto xa.$$

and, for a loop Q, the multiplication group is

$$\mathrm{Mlt}(Q) = \langle L_a, R_a;\ a \in Q \rangle .$$

An important subgroup of the multiplication group is the inner mapping group, defined as

$$\mathrm{Inn}(Q) = \mathrm{Mlt}(Q)_1 = \{\alpha \in \mathrm{Mlt}(Q);\ \alpha(1) = 1\}.$$

In groups, the inner mapping are just conjugations, i.e. inner automorphisms, and therefore all inner mappings are automorphisms. In loops, it is usually not so, for instance the 5-element loop shown in (1) has 12 automorphisms and 24 inner mappings.

A loop Q is called automorphic if every inner mapping is an automorphisms. An automorphic loop can be also defined equationally as a loop satisfying

$$(x \cdot y)\backslash(x \cdot (y \cdot (u \cdot v))) = ((x \cdot y)\backslash(x \cdot (y \cdot u))) \cdot ((x \cdot y)\backslash(x \cdot (y \cdot v))), \tag{3}$$

$$(((u \cdot v) \cdot x) \cdot y)/(x \cdot y) = (((u \cdot x) \cdot y)/(x \cdot y)) \cdot (((v \cdot x) \cdot y)/(x \cdot y)), \tag{4}$$

$$x\backslash((u \cdot v) \cdot x) = (x\backslash(u \cdot x)) \cdot (x\backslash(v \cdot x)). \tag{5}$$

The meaning of these identities is the following: the inner mapping group is generated be the mappings

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

Then (3) ensures that $L_{x,y}$ is a homomorphism, (4) ensures that $R_{x,y}$ is a homomorphism and (5) ensures that T_x is a homomorphism.

The automorphic property is important because of the following reason: a subloop of a loop Q is normal if and only if it is preserved by every inner mapping. A subloop is called characteristic if it is preserved by every automorphism. In groups, every characteristic subgroup is normal and fractions over characteristic subgroups are very important tools. In loops, characteristic subloops need not be normal, unless we work with automorphic loops.

Examples of characteristic subloops are the left, middle and right nuclei:

$$N_\lambda(Q) = \{a \in Q;\ a \cdot (x \cdot y) = (a \cdot x) \cdot y,\ \forall x, y \in Q\},$$
$$N_\mu(Q) = \{a \in Q;\ x \cdot (a \cdot y) = (x \cdot a) \cdot y,\ \forall x, y \in Q\},$$
$$N_\rho(Q) = \{a \in Q;\ x \cdot (y \cdot a) = (x \cdot y) \cdot a,\ \forall x, y \in Q\}.$$

Another example is the center:

$$Z(Q) = \{a \in N_\lambda(Q) \cap N_\mu(Q) \cap N_\rho(Q);\ a \cdot x = x \cdot a,\ \forall x \in Q\}.$$

It is easy to see that the center consists of those elements fixed by every inner mapping and hence the center is always normal unlike nuclei that are often abnormal.

3 History of automorphic loops

The study of automorphic loops commenced in the 50's by the pioneer work of R. Bruck and L. Paige [5]. They established main properties of automorphic loops:

- they are power-associative, that means one-generated subloops are associative; we can therefore define x^k, for any k, and the notions of element order and loop exponent make sense;
- $N_\lambda(Q) \subseteq N_\mu(Q)$ and $N_\rho(Q) \subseteq N_\mu(Q)$; actually $N_\lambda(Q) = N_\rho(Q)$ but it has beed proved just recently.

The autors constructed several non-trivial examples too and, last but not least, they tackled the following question: are diassociative (every two-generated subloop is a group) automorphic loops Moufang? Bruck and Paige managed to prove only a few partial results. Several years later, J. M. Osborne [28] gave an affirmative answer in the commutative case, identifying thus the class of commutative diassociative automorphic loops and the class of commutative Moufang loops.

In the next several decades, only some minor results appeared till the era of computers. Finally, in 2002 M. Kinyon, K. Kunen and J. D. Phillips [24] solved Bruck's and Paige's question for all diassociative automorphic loops. A part of the proof was computer generated—it was one of the first non-artificial problems solved by an automated prover. The reason why the result could not be proved earlier without computers is probably the nature of identities (3)–(5). For humans, they are difficult to work with but computers treat every identity the same way, no matter whether it is ugly or nice.

The modern era of automorphic loops started in April 2008 during my visit at Denver University; together with local professors P. Vojtěchovský and M. Kinyon we focused on commutative automorphic loops (CAL). We constructed many new examples of CAL and we discovered new structural properties of finite CALs. The most important was the discovery that a finite CAL splits as the product of an odd order CAL and a 2-loop, which is of order 2^k. The proof involved a lemma with a computer generated proof. The proof was then translated into a human language so, at the end, the computer intervention is not visible in the paper; however it would be extremely difficult to find the proof directly without a computer aid.

Now the study of finite CALs falls into two branches: we managed to use the idea Glauberman had for Moufang loops and we connected finite CALs of odd order with Bruck loops and then we pushed many properties of Bruck loops back to CALs. The 2-loop case did not offer any such shortcut but we found a few properties anyway. The structural results of our work are thus [19]:

- anti-automorphic inverse property, i.e. $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$,
- Lagrange's theorem for CALs,
- existence of subloops of order p, for any prime p dividing the order of the loop,
- existence of Sylow p-subloops,
- existence of Hall Π-subloops,
- solvability of odd order loops.

We continued the cooperation during my stay in Denver two years later when we proved nilpotency of finite p-loops, for every odd prime p [21].

Paralelly with the structural research we were constructing examples of CALs to strengthen or disprove hypotheses we were making [20]. The smallest non-trivial examples have 8 elements, one of them having trivial center, showing that nilpotency of finite p-loops cannot be extended to $p = 2$. Using several techniques we constructed and enumerated all CALs up to size 31. None of them was simple, which opened the question of existence of a non-associative simple finite CAL. The structural results implied that such a simple loop would be of exponent 2, if it exists.

The question of existence of a simple finite automorphic loop then attracted the attention of several researchers. First, K. Johnsson, M. Kinyon, G. Nagy and P. Vojtěchovský [23] performed an exhaustive computer search proving that no non-associative automorphic loop smaller that 2500 is simple and no commutative non-associative automorphic loop smaller that 2^{12} is simple. For non-commutative loops, the result was extended to 4096 by P. Cameron and D. Leemans; in the commutative case, A. Grishkov, M. Kinyon and G. Nagy [14] proved, using deep results about Lie algebras, that every finite CAL is solvable and therefore not simple.

In the meantime, I was studying examples of CAL. Our paper with M. Kinyon and P. Vojtěchovský brought many examples of 2-loops but only one construction of odd order loops, namely some CALs of order p^3. Later on D. A. S. de Barros, A. Grishkov and P. Vojtěchovský [3] showed by an exhaustive calculation that this list of CALs of order p^3 is complete.

Another construction of odd order CALs was presented by A. Drápal [9] but the construction was not very transparent—it was not even clear which orders admit the construction, apart of sizes $3k$, for k odd. We analysed the construction together with D. Simon [22] and we managed to translate it into a more accessible setting. It turned out that Drápal's extension of a commutative ring R (for $R \cong \mathbb{Z}_n$ or R a field) by $\mathbb{Z}_k$ exists if and only if there exists an element ζ of order k lying either in R^* or in a quadratic extension of R; moreover in the latter case the norm of ζ has to be 1. How to construct such a quadratic extension is well-known for fields but needs some non-trivial number theory knowledge for $R \cong \mathbb{Z}_n$. In particular, starting with the field $\mathbb{Z}_p$, for p odd, this construction yields loops of order kp if and only if $k \mid (p-1)$ or $k \mid (p+1)$. We also conjectured that all CALs of order pq, for p, q primes, can be constructed in this way; this hypothesis may be confirmed soon with the recent classification of Bruck loops of the same order [26].

Most constructions of CAL presented in the literature have something in common: they are semidirect products of the middle nucleus and an abelian group. J. Hora and me [17] decided to study this situation and we discovered that the semidirect product in this case has some features common with the group semidirect product, namely an inner automorphism glueing the groups. Only in CAL case, the mapping φ in $K \rtimes_\varphi H$ is the inner mapping $L_{x,y}$ – and not T_x as in groups – and therefore we need two parameters to describe the product. Moreover, in the group case the mapping $\varphi : K \to \mathrm{Aut}(H)$ has to be a homomorphism, whereas in the CAL case the mapping $\varphi : K^2 \to \mathrm{Aut}(H)$ needs not to be bilinear; actually the conditions are a little bit weaker. Anyway, if φ happens to be a bilinear form, this case is now completely understood. Furthemore, the case of $|K|$ being odd was studied in the subsequent paper [18], where I completely described the specific cases of $|K| = 3$ and $|K| = 5$.

The area of commutative automorphic loops is flourishing now; there are several papers having appeared, not only from the authors already mentioned but also from P. Csörgő [6, 7, 8], M. Aboras [1, 2], M. Greer [12] and others. There are also results on non-commutative automorphic loops, among which the most important is the paper by M. Kinyon, K. Kunen, J. D. Phillips and P. Vojtěchovský [25] – the authors showed that automorphic loops of odd orders can be associated with Bruck loops, analogously as in the commutative case. Very little is known about the even order. Since this case covers, for instance, all the symmetric groups, we cannot expect as strong results as in the commutative case, but still there is a lot of space for further investigation.

References

[1] M. Aboras: *Dihedral-like constructions of automorphic loops*, Comment. Math. Univ. Carol. **55**,3 (2014), 269–284

[2] M. Aboras, P. Vojtěchovský: *Automorphisms of Dihedral-like Automorphic Loops*, Commun. Alg. **44**,2 (2016), 613–627

[3] D. A. S. De Barros, A. Grishkov, P. Vojtěchovský: *Commutative automorphic loops of order p^3*, J. Algebra Appl. **11**,5 (2012), 15 pages

[4] D. A. S. De Barros, A. Grishkov, P. Vojtěchovský: *The free commutative automorphic 2-generated loop of nilpotency class 3*, Comm. Math. Univ. Carol. **53**,3 (2012) 321–336

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

[6] P. Csörgő: *Multiplication groups of commutative automorphic p-loops of odd order are p-groups*, J. Algebra **350** (2012), 77–83

[7] P. Csörgő: *All automorphic loops of order p^2 for some prime p are associative*, J. Algebra Appl. **12**,6 (2013), 8 pages

[8] P. Csörgő: *All finite automorphic loops have the elementwise Lagrange property*, Rocky Mountain J. Math. **45**,4 (2015), 1101–1105

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

[10] S. M. Gagola III, J. I. Hall: *Lagrange's theorem for Moufang loops*, Acta Sci. Math. Szeged **71** (2005), 45–64

[11] G. Glauberman: *On loops of odd order I*, J. Algebra **1** (1964), 374–396.

[12] M. Greer: *A Class of Loops Categorically Isomorphic to Bruck Loops of Odd Order*, Commun. in Alg. **42**,8 (2014), 3682–3697

[13] A. Grishkov, M. L. Merlini Giuliani, M. Rasskazova, L. Sabinina: *Half-isomorphisms of finite automorphic Moufang loops*, Commun. Alg. **44** (2016) 4252–4261

[14] A. Grishkov, M. K. Kinyon, G. P. Nagy: *Solvability of commutative automorphic loops*, Proceedings AMS **142**,9 (2014) 3029–3037

[15] A. Grishkov, M. Rasskazova, P. Vojtěchovský: *Automorphic loops arising from module endomorphisms*, Publ. Math. Debrecen **88**,3–4 (2016), 287–303

[16] A. Grishkov, A. V. Zavarnitsine: *Lagrange's theorem for Moufang loops*, Math. Proc. Cambridge Phil. Soc. **139**,1 (2005), 41–57

[17] J. Hora, P. Jedlička: *Nuclear semidirect product of commutative automorphic loops*, J. Alg. Appl. **13**, 1 (2014)

[18] P. Jedlička: *Odd order semidirect extensions of commutative automorphic loops*, Commentat. Mathem. Univ. Carol. **55**,4 (2014), 447–456

[19] P. Jedlička, M. Kinyon, P. Vojtěchovský: *Structure of commutative automorphic loops*, Trans. of AMS **363**,1 (2011), 365–384

[20] P. Jedlička, M. Kinyon, P. Vojtěchovský: *Constructions of commutative automorphic loops*, Commun. in Alg. **38**, 9 (2010), 3243–3267

[21] P. Jedlička, M. Kinyon, P. Vojtěchovský: *Nilpotency in automorphic loops of prime power order*, J. Alg. **350** (2012), 64–76

[22] P. Jedlička, D. Simon: *On commutative A-loops of order pq*, J. Algebra Appl. **14**,3 (2014), 20 pages

[23] K. W. Johnson, M. K. Kinyon, G. P. Nagy, P. Vojtěchovský: *Searching for small simple automorphic loops,* LMS J. Comput. Math. **14** (2011), 200–213

[24] M. K. Kinyon, K. Kunen, J. D. Phillips: *Every diassociative A-loop is Moufang*, Proc. Amer. Math. Soc. **130** (2004), 619–624

[25] M. K. Kinyon, K. Kunen, J. D. Phillips, P. Vojtěchovský: *The structure of automorphic loops*, to appear in Trans. AMS

[26] M. K. Kinyon, G. P. Nagy, P. Vojtěchovský: *Bol loops and Bruck loops of order pq,* submitted to J. Algebra

[27] G. P. Nagy: *On centerless commutative automorphic loops*, Comment. Math. Univ. Carol. **55**,4 (2014), 485–491

[28] J. M. Osborn: *A theorem on A-loops*, Proc. Amer. Math. Soc. **9** (1958), 347–349.

[29] P. Vojtěchovský: *Three lectures on automorphic loops*, Quasigroups and Related Systems **23** (2015), 129–163

2 Construction of commutative automorphic loops

Přemysl Jedlička, Michael K. Kinyon, 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 $x(x \setminus y) = y$. 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 and only if all its left inner mappings $L_{y,x}$ 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 (see already [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),
- 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 an odd 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 .

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], $N_\lambda(Q) \le N_\mu(Q)$, $N_\rho(Q) \le N_\mu(Q)$ 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) *$G \le N_\mu(Q)$.*

(iv) *Q is a group if and only if f is a translation of the group G.*

(v) *$N_\lambda(Q) \cap G = N_\rho(Q) \cap G = Z(Q) \cap G = \{x \in G;\ f(xy) = xf(y)$ for every $y \in G\}$. When Q is not a group (that is, $G = N_\mu(Q)$), then $N_\lambda(Q) = N_\rho(Q) = Z(Q) \le G$.*

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 $G \le N_\mu(Q)$.

(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, if $f(x) = xf(1)$ for every x then $f(xy) = xf(y) = f(x)y$.

(v) We have $x * (y * z) = (x * y) * z$, $x * (\overline{y} * z) = \overline{xyz} = (x * \overline{y}) * z$, $x * (y * \overline{z}) = \overline{xyz} = (x * y) * \overline{z}$, 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, $z \in G$, which holds if and only if $xf(y) = f(xy)$ for every $y \in G$. By commutativity, $N_\lambda(Q) = N_\rho(Q)$. By (iii), $N_\lambda(Q) \cap G = Z(Q) \cap G$.

Assume that Q is not a group. Suppose that $\overline{x} \in N_\lambda(Q)$. Then $f(xyz) = \overline{x} * \overline{yz} = \overline{x} * (\overline{y} * z) = (\overline{x} * \overline{y}) * z = f(xy) * z = f(xy)z$ for every $y, z \in G$, and hence (with $y = x^{-1}$), $f(z) = f(1)z$ for every $z \in G$. By (iv), Q is a group, a contradiction. Thus $N_\lambda(Q) \le G$. □

Lemma 2.2. *Let Q be a commutative loop with subloop G satisfying $G \le N_\mu(Q)$, $[Q : G] = 2$. 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 $G \le N_\mu(Q)$. 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 $\overline{x}y = \overline{1}x \cdot y = \overline{1} \cdot xy = \overline{xy}$ for every $x, y \in G$, using $G \le N_\mu(Q)$ 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 possessing a subgroup of index 2. Then $[Q : N_\mu(Q)] \le 2$ 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).

Remark 2.4. *The assumption that Q possesses a subgroup of index 2 in Corollary 2.3 is needed only when Q is a group.*

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

Proposition 2.5. *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 $N_\mu(G(f_2)) = G$ by Lemma 2.1(iii), 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 in G, 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 2.5 will be useful in the classification of commutative A-loops of order 8.

Corollary 2.6. *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 $f_2^{-1}\psi f_1 = \psi$, so $f_2^{-1}\psi f_1(1) = \psi(1) = 1$ is a square in G 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 in G. 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 square in G 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 2.7. *Let Q be a commutative loop possessing a subgroup of index* 2. *Then the following conditions are equivalent:*

(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. 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 $G \cup \overline{G}$, and where $\setminus$ is understood in $(Q, *)$. 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 in $G(f)$, 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

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

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, $f^2(x)^2 f(t)^{-1} = f^2(x)^2 t^{-2} = f(f(x))f(f(x))t^{-2} = f(f(x)f(x))t^{-1} = f(f(x)^2)t^{-1} = f(x)^2$, 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 $g(x^2) = x^2$ and t is a fixed point of g (not necessarily satisfying $t = f(1)$). Then $f(1) = g(1)t = t$, $f(xy) = g(xy)t = g(x)g(y)t = g(x)tg(y)tt^{-1} = f(x)f(y)t^{-1}$, $f(x^2) = g(x^2)t = x^2t$, 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 2.7, 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 2.5, Corollary 2.6 and Proposition 2.7.

Lemma 3.1. *Let G be a commutative loop, $1 \neq g \in \mathrm{Aut}(G)$ 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, and $Z(G(g)) = \{x \in G;\ g(x) = x\}$.*

Proof. Since g is not a translation of G, neither is f. Hence both $G(g)$ and $G(f)$ are nonassociative, by Lemma 2.1(iv). By Lemma 2.1(v), $Z(G(f)) = \{x \in G;\ f(xy) = xf(y)$ for every $y \in G\} = \{x \in G;\ g(xy)t = xg(y)t$ for every $y \in G\} = \{x \in G;\ g(xy) = xg(y)$ for every $y \in G\} = Z(G(g))$ and it is also equal to $\{x \in G;\ g(x) = x\}$ since $g(xy) = g(x)g(y)$. □

Let Q be a nonassociative commutative A-loop of order 8, necessarily with a middle nucleus of index 2. By Proposition 2.7, $Q = G(f)$, 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 $f(x) = g(x)t = xt$ for some $t \in G$. Then $G(f)$ is a commutative group by Lemma 2.1(iv). 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 2.6(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 $\mathrm{Aut}(G) = \{1, (a, b), (a, ab), (b, ab), (a, b, ab), (a, ab, b)\} \cong S_3$. The only square in G is 1 and it is trivially fixed by all $g \in \mathrm{Aut}(G)$.

If $g = 1$ and $f(x) = g(x)t = xt$ for some $t \in G$, $G(g)$ is a commutative group by Lemma 2.1(iv). Let $g_1 = (a, b)$. 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 $G(g_1) \ncong G(f_1)$.

Let $g_2 = (a, ab)$, 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 2.6(i). Note that $f_1 = \psi^{-1} f_2 \psi$ with $\psi = (b, ab)$. Hence $G(f_1) \cong G(f_2)$ by Corollary 2.6. 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 3.1, $Z(G(g_4)) = 1$ and $Z(G(f_1)) = Z(G(g_1)) \cong \mathbb{Z}_2$. 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 2.6(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 $\{e_1, \dots, e_n\}$ 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 $g(x + x) = g(0) = 0 = g(x) + g(x)$, the equivalence of (i) and (iv) in Proposition 2.7 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 3.1 implies that $Z(Q_n) = 1$, 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 [5, 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 [5, 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 $g(y,x,z)=g(y,z,x)$ for every x, z, that is, if and only if the induced bilinear form $g(y,-,-):V^2\to\mathrm{GF}(2)$ is symmetric.

Lemma 4.4. *Let V be a vector space over $\mathrm{GF}(2)$ of dimension at least 3. Then there exists a trilinear form $g:V\to\mathrm{GF}(2)$ such that for any $0\neq x\in V$ the induced bilinear form $g(x,-,-):V^2\to\mathrm{GF}(2)$ is not symmetric.*

Proof. Let $\{e_1,\dots,e_n\}$ be a basis of V. The trilinear form g is determined by the values $g(e_i,e_j,e_k)\in\mathrm{GF}(2)$, for $1\leq i,j,k\leq n$. Set $g(e_i,e_i,e_{i+1})=1$ for every i (with $e_{n+1}=e_1$) and $g(e_i,e_j,e_k)=0$ otherwise.

Let $x=\sum\alpha_je_j$ be such that $\alpha_i\neq 0$ for some i. Then $g(x,e_i,e_{i+1})=\sum\alpha_jg(e_j,e_i,e_{i+1})=\alpha_ig(e_i,e_i,e_{i+1})=\alpha_i\neq 0$, while, similarly, $g(x,e_{i+1},e_i)=0$. □

Example 4.5. *By Lemma 4.4, 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 4.6. *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 4.5. 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 §, and the parameters $(4,2)$ are possible (see §). Then (k,ℓ) can be achieved using the appropriate direct product.

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

We remark that Lemma 4.4 cannot be improved:

Lemma 4.7. *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 4.8. *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 4.9. *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 4.10. *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

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

Then

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

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 4.11. *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 $Q_\theta = K \bowtie_\theta Z$, $Q_{\mu\theta} = K \bowtie_{\mu\theta} Z$ 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 4.10. 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

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

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, in particular a Bol 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 nonassociative 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 Proposition 5.1, $Q/Z(Q)$ 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 $0 \le i < p$ and $z \in Z(Q)$. With $0 \le i, j, k < p$ 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, in fact, that the center must have size p if p is odd.)

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

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

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

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

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 $Q_{a,b}(\mathbb{Z}_n)$ on $\mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n$ by

$$(x_1, x_2, x_3)(y_1, y_2, y_3) = (x_1 + y_1 + (x_2 + y_2)x_3y_3 + a(x_2, y_2)_n + b(x_3, y_3)_n, x_2 + y_2, x_3 + y_3). \tag{5.3}$$

Then $Q_{a,b}(\mathbb{Z}_n)$ can be seen as a central extension of $\mathbb{Z}_n$ by $\mathbb{Z}_n \times \mathbb{Z}_n$ via the loop cocycle $\theta((x_2, x_3), (y_2, y_3)) = (x_2 + y_2)x_3y_3 + a(x_2, y_2)_n + b(x_3, y_3)_n$, and hence $Q_{a,b}(\mathbb{Z}_n)$ is a commutative loop with neutral element $(0, 0, 0)$.

Note that we can write θ as $\theta = \mu + \nu$, where $\mu((x_2, y_2), (x_3, y_3)) = (x_2 + y_2)x_3y_3$ 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 $Q = Q_{a,b}(\mathbb{Z}_n)$ 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) $x \setminus y = (y_1 - x_1 - (y_3 - x_3)x_3y_2 - a(x_2, y_2 - x_2)_n - b(x_3, y_3 - x_3)_n, y_2 - x_2, y_3 - x_3)$,

(ii) $L_{y,x}(z) = xy \setminus x(yz) = (z_1 + y_3(x_3z_2 - x_2z_3), z_2, z_3)$,

(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 $m \geq 0$, $x^m = (mx_1 + 2\binom{m+1}{3}x_2x_3^2 + at_2 + bt_3, mx_2, mx_3)$, where $t_i = \sum_{k=1}^{m-1}(x_i, kx_i)_n$. (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 $Q_0 = Q_{0,0}(\mathbb{Z}_n)$. By Lemma 4.10, it suffices to verify the formula (ii) for Q_0 instead of 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 4.11, 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 are consequences of 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 suffices to show that $(0, 0, x_3) \notin N_\mu(Q_0)$ 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

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

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),

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

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 on 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 $Q = Q_{a,b}(\mathbb{Z}_p)$. 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). □

As usual, denote by $\mathbb{Z}_n^*$ the set of all invertible elements of $\mathbb{Z}_n$.

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

Proof. Define $\varphi : Q_{0,b}(\mathbb{Z}_n) \to Q_{0,c}(\mathbb{Z}_n)$ 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 $Q_{0,b}(\mathbb{Z}_n)$ and by $*$ the multiplication in $Q_{0,c}(\mathbb{Z}_n)$. 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*. Also recall 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 $Q_{a_1,0}(\mathbb{Z}_p) \cong Q_{a_2,0}(\mathbb{Z}_p)$.*

Proof. Since $a_1 a_2^{-1}$ is a quadratic residue, there is u such that $a_2 = a_1 u^2$. Define $\varphi : \mathcal{Q}_{a_1,0}(\mathbb{Z}_p) \to \mathcal{Q}_{a_2,0}(\mathbb{Z}_p)$ by $(x_1, x_2, x_3) \mapsto (u^2 x_1, x_2, u x_3)$. 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

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

□

Lemma 5.8. *For a prime p, let $Q_1 = \mathcal{Q}_{a,b}(\mathbb{Z}_p) = (Q_1, \cdot)$, $Q_2 = \mathcal{Q}_{a,c}(\mathbb{Z}_p) = (Q_2, *)$ 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 $x_3 < p$. 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 Lemma 5.5 and Corollary 5.10, 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 $0\leq b<p\}$ and $I_n=\{\mathcal{Q}_{a,b}(\mathbb{Z}_p);\ a>0$ is a quadratic nonresidue modulo p and $0\leq b<p\}$ 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 $\mathcal{Q}_{0,0}(\mathbb{Z}_3)\to\mathcal{Q}_{0,1}(\mathbb{Z}_3)$, $f_{(0,0,2)}$ 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.

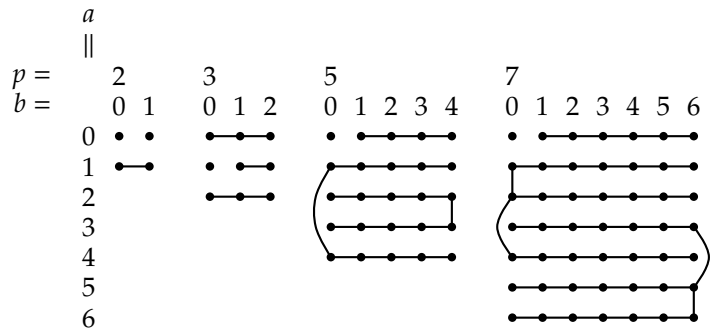

Figure 1: Isomorphism classes of loops $Q_{a,b}(\mathbb{Z}_p)$ for $p \in \{2, 3, 5, 7\}$.

Altogether, Figure 1 depicts the isomorphism classes of loops $Q_{a,b}(\mathbb{Z}_p)$ 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 $Q_{a,b}(\mathbb{Z}_p)$.

Using a linear-algebraic approach to cocycles (see Subsection), 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 $Q_{a,b}(\mathbb{Z}_p)$. 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 $Q_{a,b}(\mathbb{Z}_p)$ 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.

Table 1: Commutative A-loops up to isomorphism (up to isotopism).

n	8	15	16	21	24	27	30	32
groups	3	1	5	1	3	3	1	7
nonassociative loops	4(3)	1	46(38)	1	4(3)	4	1	?
nonassociative loops with nontrivial center	3(2)	0	44(37)	0	4(3)	4	1	?
nonassociative loops of exponent p	2	–	12(11)	–	–	0	–	?
nonassociative loops of exponent p with nontrivial center	1	–	10	–	–	0	–	211(210)

If there is only one number in a cell of the table, 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.

6.1 Comments on commutative A-loops of order 8

For classification up to isomorphism, see Section .

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 $\alpha(x) = x$, $\alpha(\overline{x}) = \overline{xz^{-1}}$, $\beta(x) = zx$, $\beta(\overline{x}) = \overline{x}$, $\gamma(x) = zx$, and $\gamma(\overline{x}) = \overline{x}$. Then

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

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 , 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 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 $\theta,\ \mu : K \times K \to Z$ 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 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 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 with LOOPS.

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 .

7 Acknowledgement

We thank the anonymous referee for the nice proof of Lemma 4.4.

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, 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*, Comment. Math. Univ. Carolin. **49** (2008), 357–382.

[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*, Trans. Amer. Math. Soc. **363**,1 (2011), 365–384

[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.

3 The structure of commutative automorphic loops

Přemysl Jedlička, Michael K. Kinyon, Petr Vojtěchovský

Abstract

An *automorphic loop* (or *A-loop*) is a loop whose inner mappings are automorphisms. Every element of a commutative A-loop generates a group, and $(xy)^{-1} = x^{-1}y^{-1}$ holds. Let Q be a finite commutative A-loop and p a prime. The loop Q has order a power of p if and only if every element of Q has order a power of p. The loop Q decomposes as a direct product of a loop of odd order and a loop of order a power of 2. If Q is of odd order, it is solvable. If A is a subloop of Q then $|A|$ divides $|Q|$. If p divides $|Q|$ then Q contains an element of order p. If there is a finite simple nonassociative commutative A-loop, it is of exponent 2.

1 Introduction

A *loop* $(Q, \cdot)$ is a set Q with a binary operation $\cdot$ such that (i) for each $x \in Q$, the *left translation* $L_x : Q \to Q; y \mapsto yL_x = xy$ and the *right translation* $R_x : Q \to Q; y \mapsto yR_x = yx$ are bijections, and (ii) there exists $1 \in Q$ satisfying $1 \cdot x = x \cdot 1 = x$ for all $x \in Q$. The left and right translations generate the *multiplication group* $\mathrm{Mlt}(Q) = \langle L_x, R_x \mid x \in Q \rangle$. The *inner mapping group* $\mathrm{Inn}(Q) = \mathrm{Mlt}(Q)_1$ is the stabilizer of $1 \in Q$. Standard references for the theory of loops are [4, 5, 17].

A loop Q is an *automorphic loop* (or *A-loop*) if every inner mapping of Q is an automorphism of Q, that is, $\mathrm{Inn}(Q) \leq \mathrm{Aut}(Q)$. Thus the class of A-loops, which is certainly not the class of all loops, includes, for instance, groups and commutative Moufang loops [5].

The study of A-loops was initiated by Bruck and Paige [6]. They obtained many basic structural results for A-loops and also described some constructions. The bulk of [6] was devoted to the (implicitly stated) problem of whether every *diassociative* A-loop, that is, an A-loop in which every 2-generated subloop is a group, is a Moufang loop. Affirmative answers were given by Osborn [16] in the commutative case, and Kinyon, Kunen and Phillips [13] in the general case. Moufang A-loops have been used to characterize a certain class of quasigroups [12], and have been shown to have an affirmative answer for the restricted Burnside problem [18].

By contrast, the study of other classes of A-loops has lain quite fallow. In this paper, we give a detailed structure theory for *commutative* A-loops. Here is a summary of our main results:

In §2, we present preliminary results which will be used throughout the rest of the paper. Some of these results, such as the power-associativity of commutative A-loops (Lemma 2.4) are already known for arbitrary A-loops [6], but we give short proofs to make the present paper self-contained. Other results, such as the automorphic inverse property (Lemma 2.6) are new.

In §3, we study commutative A-loops of odd order, i.e. finite A-loops in which every element has odd order (Lemma 3.1). The multiplication group of a commutative A-loop contains a natural (but not at all obvious) twisted subgroup (Lemma 3.3). In the odd order case, this enables us to construct a new loop operation on a commutative A-loop with the property that powers in the new loop coincide with powers in the original loop (Lemma 3.5). The new loop is in fact a *Bruck loop*, and we exploit this fact to establish *Lagrange* and *Cauchy* theorems for commutative A-loops of odd order (Propositions 3.6 and 3.7). Our main result in §3 is the *Odd Order Theorem*: every commutative A-loop of odd order is solvable (Theorem 3.12).

In §4, we turn to a property trivially satisfied in abelian groups and valid in commutative Moufang loops thanks to dissociativity: the product of squares is a square. This turns out be true in commutative A-loops as well (Theorem 4.1), despite the fact that the naive formula $x^2y^2 = (xy)^2$ does not hold in general. Instead, $x^2y^2 = (x \diamond y)^2$ for a rather complicated binary operation $\diamond$; in the Moufang case, $\diamond$

coincides with the original operation. Following the same philosophy as in the odd order case, we study the new operation $\diamond$ and note that it defines a commutative, power-associative loop on the same underlying set as the original commutative A-loop. In the odd order case, $\diamond$ yields an isomorphic copy of the original loop (Lemma 4.6), but at the other extreme where every element has order a power of 2, the new loop operation $\diamond$ turns out to have strong structural properties, as we will show in later sections.

In §5, we prove a *Decomposition Theorem*: every finite commutative A-loop is a direct product of a subloop of odd order and a subloop in which every element has order a power of 2 (Theorem 5.1). This is a generalization of the familiar decomposition theorems in abelian groups and commutative Moufang loops. Unlike in those cases, however, no further decomposition is possible: commutative A-loops of odd order are not necessarily direct products of p-loops for odd p.

In §6, we examine commutative A-loops of exponent 2. This special case is of particular importance because of a straightforward consequence of the Decomposition Theorem and the Odd Order Theorem, namely that a finite, simple, commutative A-loop is either a cyclic group of odd prime order or it has exponent 2 (Proposition 6.1). To study the exponent 2 case, we return to the new loop operation $\diamond$ introduced in §4, and prove the main result of §6: if Q is a finite, commutative A-loop of exponent 2, then $(Q, \diamond)$ is an elementary abelian 2-group (Theorem 6.2). An immediate corollary of this is that a commutative A-loop of exponent 2 has order a power of 2 (Corollary 6.3).

In §7, we briefly examine p-loops. The main result is that the two reasonable definitions of this notion coincide for commutative A-loops, that is, a finite commutative A-loop has order a power of p if and only if every element has order a power of p (Theorem 7.1). For p odd, this is a consequence of the Lagrange and Cauchy theorems. For $p = 2$, it follows from the Decomposition Theorem and the fact that it has already been observed in the exponent 2 case. We now easily derive the *Lagrange* and *Cauchy Theorems* for all finite commutative A-loops (Theorem 7.2).

Finally, in §8 we state three open problems. The first, which we expect to generate a great deal of interest in loop theory, is whether there exists a nonassociative, finite simple commutative A-loop (Problem 8.1). The results in this paper already tell us a great deal about the structure such a loop must have. The second problem (Problem 8.2) is whether every commutative A-loop of odd prime power order has a nontrivial center, that is, whether the loop is centrally nilpotent. The third (Problem 8.3) addresses the existence of Hall and Sylow subloops.

We should note that the variety of commutative A-loops is vast compared to the variety of abelian groups. There exist many nonassociative examples even under very restrictive conditions, such as in the case of commutative A-loops of exponent two. While every A-loop of prime order p is isomorphic to the cyclic group of order p, a class of nonassociative commutative A-loops of order pq ($2 < p < q$ primes) was found by Drápal [7]. A survey of known constructions and the classification of commutative A-loops of small orders will appear in the planned sequel [11] to this paper. In [11], we also give an example of a commutative A-loop of order 16 that is not centrally nilpotent.

The main idea of this paper is to associate a new loop operation with the original loop. In the odd order case, where the original loop is uniquely 2-divisible, this is a familiar approach [10], [8]. However, in all earlier instances it was somewhat transparent what the associated loop operation should be, unlike here. A common feature is to take advantage of the unique square roots. We do not have access to square roots in 2-loops, but if for every x, y there is z such that $x^2y^2 = z^2$ (Theorem 4.1), our novel idea is to declare z to be a new product of x and y. As demonstrated in this paper, this approach is most fruitful in case of commutative A-loops. Moreover, we now have some anecdotal evidence that the connection is more profound, and that binary operations associated in this or similar manner are deserving of a systematic investigation in other varieties of loops.

The well-behaved structure theory of commutative A-loops belies the rather technical lemmas on which it is based. Most of these lemmas involve detailed equational reasoning, often obtained with the assistance of the automated theorem prover Prover9 [15].

Finally, we should mention that many of our structural results for commutative A-loops of odd order can be generalized to the noncommutative case. These generalizations will appear elsewhere

[14].

1.1 Notation

Throughout the paper, let Q denote a commutative loop with multiplication denoted by juxtaposition and with neutral element 1. Since all left translations are bijections of Q, it is convenient to define the associated left division operation by

$$x \setminus y = yL_x^{-1}$$

for all $x, y \in Q$. It will also be useful to introduce the *division permutations* $D_x : Q \to Q$, $x \in Q$, defined by

$$yD_x = y \setminus x = xL_y^{-1}$$

for all $x, y \in Q$. Note that $D_x^2 = \mathrm{id}\, Q$ for all $x \in Q$. We will use the usual notation $x^{-1} = x \setminus 1$ for the inverse of x, and we will also use the *inversion permutation* $J : Q \to Q$ defined by

$$xJ = xD_1 = x^{-1}$$

for all $x \in Q$.

To avoid excessive parenthesization, we will use the following convention. The multiplication operation $\cdot$ will be less binding than left division, which is, in turn, less binding than juxtaposition. For example, with this convention, $ab \setminus cd \cdot g \setminus ef$ is unambiguously read as $((ab) \setminus (cd))(g \setminus (ef))$. On the other hand, we shall certainly use parentheses, brackets, *etc.*, whenever they help to clarify an expression.

It is well known [5] that for commutative loops, the inner mapping group $\mathrm{Inn}(Q)$ has a distinguished set of generators

$$L_{x,y} = L_x L_y L_{yx}^{-1}$$

for $x, y \in Q$. Using these generators, the A-loop condition can be expressed as follows:

$$(uv)L_{x,y} = uL_{x,y} \cdot vL_{x,y}\,. \tag{A}$$

It follows from (A) that $(u \setminus v)L_{x,y} = uL_{x,y} \setminus vL_{x,y}$ and also $JL_{x,y} = L_{x,y}J$.

The assertion that a permutation φ of a loop Q is an automorphism of Q can be expressed in equivalent ways in terms of the various loop permutations:

$$L_x\varphi = \varphi L_{x\varphi}, \qquad D_x\varphi = \varphi D_{x\varphi}\,.$$

We shall use these in calculations while referencing (A).

2 Preliminaries

In this section, we establish several preliminary results for commutative A-loops which will be needed later. Some of these generalize rather easily to arbitrary A-loops, and some of those generalizations can be found in [6]. We give brief proofs in the commutative case to make the paper self-contained.

For an automorphism φ of a loop Q, let $\mathrm{Fix}(\varphi) = \{x \in Q \mid x\varphi = x\}$. We begin with an easy observation.

Lemma 2.1. *Let Q be a loop and let $\varphi \in \mathrm{Aut}(Q)$. Then*

i) $\mathrm{Fix}(\varphi)$ *is a subloop,*

ii) *If $x \in \mathrm{Fix}(\varphi)$, then $\langle x \rangle \leq \mathrm{Fix}(\varphi)$,*

iii) *For each $x \in \mathrm{Fix}(\varphi)$,*

$$L_x\varphi = \varphi L_x \qquad \text{and} \qquad D_x\varphi = \varphi D_x\,. \tag{2.1}$$

Lemma 2.2. *For all x, y, z in a commutative A-loop Q,*

$$x \in \mathrm{Fix}(L_{y,z}) \qquad \Leftrightarrow \qquad yL_xL_z = yL_zL_x \qquad \Leftrightarrow \qquad z \in \mathrm{Fix}(L_{y,x})\,.$$

Proof. We have $xL_{y,z} = x$ iff $xL_yL_z = xL_{yz}$ iff $yL_xL_z = yL_zL_x$. Since this last equation is symmetric in x and z, the other equivalence follows. □

For x in a loop Q and $n \in \mathbb{Z}$, we define $x^n = 1L_x^n$. Then $x \cdot x^n = 1L_x^nL_x = 1L_x^{n+1} = x^{n+1}$ for all $n \in \mathbb{Z}$. Also, for any $\varphi \in \mathrm{Aut}(Q)$, $(x^n)\varphi = 1L_x^n\varphi = 1\varphi L_{x\varphi}^n = (x\varphi)^n$.

Lemma 2.3 ([6], Thm 2.6)**.** *In a commutative A-loop, the following identities hold for all x, y and for all $m, n \in \mathbb{Z}$:*

$$x^nL_{y,x^m} = x^n \tag{2.2}$$
$$L_{x^m}L_{x^n} = L_{x^n}L_{x^m} \tag{2.3}$$
$$L_{x^n}L_{y,x^m} = L_{y,x^m}L_{x^n} \tag{2.4}$$
$$D_{x^n}L_{y,x^m} = L_{y,x^m}D_{x^n} \tag{2.5}$$

Proof. First, we have $xL_{y,x} = xy \setminus (x \cdot yx) = xy \setminus (xy \cdot x) = x$, so that $x \in \mathrm{Fix}(L_{y,x})$. By (A) and Lemma 2.1(ii), $x^n \in \mathrm{Fix}(L_{y,x})$ for all $n \in \mathbb{Z}$. Thus by Lemma 2.2, $x \in \mathrm{Fix}(L_{y,x^n})$, and so $x^m \in \mathrm{Fix}(L_{y,x^n})$ for all $m, n \in \mathbb{Z}$ by (A) and Lemma 2.1(ii) again. This establishes (2.2), and then (2.3) follows from another application of Lemma 2.2. Finally, (2.4) and (2.5) follow from (2.2) and (2.1). □

A loop is said to be *power-associative* if for each x, the subloop $\langle x \rangle$ is a group. Power-associativity is equivalent to $x^mx^n = x^{m+n}$ for all $x \in Q$ and all $m, n \in \mathbb{Z}$.

Lemma 2.4 ([6], Thm. 2.4)**.** *Every commutative A-loop is power-associative.*

Proof. For all $m, k \in \mathbb{Z}$ and for all x,

$$x^mx^{k+1} = x^m(x^k \cdot x) \overset{(2.4)}{=} x^k(x^m \cdot x) = x^{m+1}x^k\,.$$

By an easy induction, $x^mx^{k+n} = x^{m+n}x^k$ for all $m, n, k \in \mathbb{Z}$. Taking $k = -n$, we have the desired result. □

Lemma 2.5. *In a commutative A-loop, the following identities hold:*

$$y^nL_{y,x} = (xy \setminus x)^{-n} \qquad \text{for all } n \in \mathbb{Z}\,, \tag{2.6}$$
$$xy^2 = (xy)(xy \setminus x)^{-1}\,. \tag{2.7}$$

Proof. We compute

$$y^{-n}L_{y,x} = (y^{-1})^nL_{y,x} \overset{(A)}{=} (y^{-1}L_{y,x})^n = (xy \setminus x)^n\,,$$

and thus obtain (2.6) upon replacing n with $-n$. Finally we have

$$xy \setminus xy^2 = yL_{y,x} \overset{(2.6)}{=} (xy \setminus x)^{-1}\,,$$

which is equivalent to (2.7). □

A loop is said to have the *automorphic inverse property* (AIP) if it has two-sided inverses and satisfies

$$(xy)^{-1} = x^{-1}y^{-1} \qquad \text{or equivalently,} \qquad L_xJ = JL_{x^{-1}} \tag{AIP}$$

for all x, y.

Lemma 2.6. *Every commutative A-loop has the AIP.*

Proof. Using the fact that $L_{x^{-1}}L_x = L_{x^{-1},x}$ is an automorphism, we compute

$$\begin{aligned} yL_xL_{x^{-1}}J &\overset{(2.3)}{=} yL_{x^{-1}}L_xJ & &\overset{(A)}{=} y^{-1}L_{x^{-1}}L_x \\ &= x^{-1}[L_{y^{-1}}L_y^{-1}][L_yL_x] & &\overset{(2.3)}{=} x^{-1}L_y^{-1}[L_{y^{-1}}L_{y,x}]L_{xy} \\ &\overset{(A)}{=} x^{-1}L_y^{-1}L_{y,x}L_{y^{-1}L_{y,x}}L_{xy} & &\overset{(2.6)}{=} [(xy)^{-1}\cdot(xy\setminus x)]L_{xy} \\ &= xL_{xy}^{-1}L_{(xy)^{-1}}L_{xy} & &\overset{(2.3)}{=} xL_{(xy)^{-1}} \\ &= (xy)^{-1}L_x & &= yL_xJL_x\,. \end{aligned}$$

Thus $L_xL_{x^{-1}}J = L_xJL_x$, or $L_{x^{-1}}J = JL_x$. Replacing x with x^{-1}, we obtain (AIP). □

Lemma 2.7. *In a commutative A-loop, the following identities hold.*

$$L_{x,y} = L_{x^{-1},y^{-1}} \tag{2.8}$$

$$L_{x,y} = L_{x^{-1}\setminus y}^{-1}L_xL_y \tag{2.9}$$

$$L_{x,y} = L_yL_{x^{-1}\setminus y}^{-1}L_x \tag{2.10}$$

$$L_{x\setminus y,x} = L_{(y\setminus x)^{-1},x} \tag{2.11}$$

$$L_{(x\setminus y)^{-1}\setminus x}^{-1}L_{x\setminus y} = L_y^{-1}L_{y\setminus x} \tag{2.12}$$

Proof. First, (2.8) is an easy consequence of the AIP:

$$\left(zL_{x,y}\right)^{-1} \overset{(AIP)}{=} z^{-1}L_{x^{-1},y^{-1}} \overset{(A)}{=} \left(zL_{x^{-1},y^{-1}}\right)^{-1}\,.$$

For (2.9), we compute

$$\begin{aligned} L_{x^{-1}\setminus y}^{-1}[L_xL_y] &= [L_{x^{-1}\setminus y}^{-1}L_{x,y}]L_{yx} & &\overset{(A)}{=} L_{x,y}L_{(x^{-1}\setminus y)L_{x,y}}^{-1}L_{yx} \\ &\overset{(2.8)}{=} L_{x,y}L_{(x^{-1}\setminus y)L_{x^{-1},y^{-1}}}^{-1}L_{yx} & &= L_{x,y}L_{(y^{-1}x^{-1})^{-1}}^{-1}L_{yx} \\ &\overset{(AIP)}{=} L_{x,y}L_{yx}^{-1}L_{yx} & &= L_{x,y}\,. \end{aligned}$$

Next, we have

$$L_y^{-1}L_{x,y} \overset{(2.4)}{=} L_{x,y}L_y^{-1} \overset{(2.9)}{=} L_{x^{-1}\setminus y}^{-1}L_x\,,$$

which gives (2.10). For (2.11), we compute

$$L_{x\setminus y,x} = L_{x\setminus y,x}^{-1}L_{x\setminus y,x}^2 \overset{(A)}{=} L_{x\setminus y,x}^{-1}L_{x\setminus y,x}L_{x\setminus y,x}L_{(x\setminus y)L_{x\setminus y,x}xL_{x\setminus y,x}} = L_{(y\setminus x)^{-1},x}$$

using (2.6) and (2.2). Finally, we apply (2.9) to both sides of (2.11) to get

$$L_{(x\setminus y)^{-1}\setminus x}^{-1}L_{x\setminus y}L_x = L_{(y\setminus x)\setminus x}^{-1}L_{y\setminus x}L_x\,.$$

Canceling and using $(y\setminus x)\setminus x = y$, we obtain (2.12). □

Lemma 2.8. *For all x, y in a commutative A-loop,*

$$D_{x^2} = D_xJD_x \tag{2.13}$$

$$x^2 = yD_x\cdot y^{-1}D_x \tag{2.14}$$

$$x = y^{-1}D_{x^{-1}}\cdot yD_{x^2}\,. \tag{2.15}$$

Proof. For all x, y,

$$\begin{aligned} yD_{x^2} &= xL_xL_y^{-1} && = xL_{x\backslash y}^{-1}[L_{x\backslash y}L_xL_{x\cdot x\backslash y}^{-1}] && = xL_{x\backslash y}^{-1}L_{x\backslash y,x} \\ &\overset{(A)}{=} xL_{x\backslash y,x}L_{(x\backslash y)L_{x\backslash y,x}}^{-1} && \overset{(2.6)}{=} xL_{x\backslash y,x}L_{(y\backslash x)^{-1}}^{-1} && \overset{(2.2)}{=} xL_{(y\backslash x)^{-1}}^{-1} \\ &= (y\backslash x)^{-1}D_x && = yD_xJD_x\,. \end{aligned}$$

This establishes (2.13). Rewrite (2.13) as $JD_x = D_xD_{x^2}$ since $D_x^{-1} = D_x$. Applying this to y, we have $y^{-1}D_x = yD_xD_{x^2} = x^2L_{yD_x}^{-1}$, which is equivalent to (2.14). Finally, rewrite (2.13) (applied to y) as $xL_{yD_xJ}^{-1} = yD_{x^2}$, or $x = yD_{x^2}L_{yD_xJ}$. Using (AIP), we obtain (2.15). □

3 Commutative A-loops of odd order

A loop is *uniquely* 2*-divisible* if the squaring map $x \mapsto x^2$ is a permutation. In finite, power-associative loops, being uniquely 2-divisible is equivalent to each element having odd order.

The following is well-known and holds in more generality than we need here.

Lemma 3.1. *A finite commutative loop Q is uniquely* 2*-divisible if and only if it has odd order.*

Proof. If Q is uniquely 2-divisible, then the inversion permutation J does not fix any nonidentity elements. Hence the set of nonidentity elements of Q has even order, and so Q has odd order.

Now assume Q has odd order, and fix $c \in Q$. By commutativity, the set $U = \{(x, y) \,|\, xy = c, x \neq y\}$ has even order. Since the set $V = \{(x, y) \,|\, xy = c\}$ has size $|Q|$, it follows that the set $U\backslash V = \{(x, x) \,|\, x^2 = c\}$ has odd order, and hence is nonempty. Thus the squaring map $x \mapsto x^2$ is surjective, and hence, by finiteness, bijective. □

In this section we will study the structure of commutative A-loops of odd order in detail. To explain our approach, we first need a useful notion from group theory; *cf.* [3, 8].

A *twisted subgroup* of a group G is a subset $T \subset G$ satisfying (i) $1 \in T$, (ii) $a^{-1} \in T$ for each $a \in T$, and (iii) $aba \in T$ for each $a, b \in T$. A twisted subgroup T is uniquely 2-divisible if the restriction of the squaring map $x \mapsto x^2$ to T is a permutation.

On a uniquely 2-divisible twisted subgroup T, one can define a loop operation $\circ$ by $a \circ b = (ab^2a)^{1/2}$ where the exponent $1/2$ denotes the unique square root in T. The loop $(T, \circ)$ is then a (left) *Bol loop*, that is, it satisfies the identity $x \circ (y \circ (x \circ z)) = (x \circ (y \circ x)) \circ z$. In addition, $(T, \circ)$ satisfies (AIP); left Bol loops with (AIP) are known as left *Bruck loops*.

For some classes of loops, the multiplication groups contain natural twisted subgroups. Up until now, the only known example of this is the variety of Bol loops: for a Bol loop Q, the set $L_Q = \{L_x \,|\, x \in Q\}$ of left translations is a twisted subgroup of $\mathrm{Mlt}(Q)$. In case Q is uniquely 2-divisible, there is also a natural left Bruck loop structure on L_Q. It turns out that this Bruck loop structure can be isomorphically transferred to the underlying set Q itself, so that Q has two loop structures (which may or may not coincide); its original Bol loop structure and the transferred Bruck loop structure.

There are two things that make all of this particularly useful. The first is that uniquely 2-divisible Bruck loops are highly structured [9]. The second is that powers of elements in the two loop structures coincide. It is thus possible to prove results about the original Bol loop by using its associated Bruck loop. This idea was fruitfully exploited for Moufang loops by Glauberman [10]; for the Bol case, see [8].

We will now apply the same circle of ideas to commutative A-loops. We will start by identifying a twisted subgroup of the multiplication group of a commutative A-loop. For each x in a commutative A-loop Q, set

$$P_x = L_xL_{x^{-1}}^{-1} \overset{(2.3)}{=} L_{x^{-1}}^{-1}L_x\,. \tag{P}$$

and let $P_Q = \{P_x \,|\, x \in Q\}$. Observe that the set P_Q trivially satisfies two of the conditions for being a twisted subgroup: $\mathrm{id}\, Q = P_1 \in P_Q$, and for each $x \in Q$,

$$P_x P_{x^{-1}} = L_x L_{x^{-1}}^{-1} L_{x^{-1}} L_x^{-1} = \mathrm{id}\, Q\,,$$

so that $P_x^{-1} = P_{x^{-1}} \in P_Q$.

Lemma 3.2. *For all x, y in a commutative A-loop Q,*

$$x^{-1} P_{xy} = xy^2 \tag{3.1}$$

$$L_{x^{-1}} P_{xy} = P_y L_x \tag{3.2}$$

Proof. Applying (AIP) to (2.7) and rearranging gives (3.1). Next, for all $x, y \in Q$,

$$\begin{aligned} L_{x^{-1}} P_{xy} &= L_{x^{-1}} L_{(xy)^{-1}}^{-1} L_{xy} \overset{(\mathrm{AIP})}{=} L_{x^{-1}} L_{x^{-1}y^{-1}}^{-1} L_{xy} = L_{y^{-1}}^{-1} L_{y^{-1},x^{-1}} L_{xy} \\ &\overset{(2.8)}{=} L_{y^{-1}}^{-1} L_{y,x} L_{xy} \quad = L_{y^{-1}}^{-1} L_y L_x \qquad = P_y L_x\,. \end{aligned}$$

This proves (3.2). □

Note that (3.1) can also be obtained by applying (3.2) to $1 \in Q$.

Lemma 3.3. *For all x, y in a commutative A-loop Q,*

$$P_x P_y P_x = P_{yP_x}\,. \tag{3.3}$$

In particular, P_Q is a twisted subgroup of $\mathrm{Mlt}(Q)$.

Proof. For all $x, y \in Q$,

$$\begin{aligned} P_x P_y P_x &= P_x P_y L_x L_{x^{-1}}^{-1} &&\overset{(3.2)}{=} P_x L_{x^{-1}} P_{xy} L_{x^{-1}}^{-1} \\ &\overset{(\mathrm{P})}{=} L_x P_{xy} L_{x^{-1}}^{-1} &&= L_x P_{x^{-1}(x^{-1} \setminus xy)} L_{x^{-1}}^{-1} \\ &\overset{(\mathrm{P})}{=} L_x P_{x^{-1} \cdot yP_x} L_{x^{-1}}^{-1} &&\overset{(3.2)}{=} P_{yP_x} L_{x^{-1}} L_{x^{-1}}^{-1} \\ &= P_{yP_x}\,. \end{aligned}$$

This establishes (3.3), and the rest follows immediately. □

Lemma 3.4. *For all x in a commutative A-loop Q and for all $n \in \mathbb{Z}$,*

$$P_x^n = P_{x^n}\,. \tag{3.4}$$

Proof. We have already noted (3.4) for $n = -1$, while it is trivial for $n = 0, 1$. If (3.4) holds some n, then

$$P_x^{n+2} = P_x P_{x^n} P_x \overset{(3.3)}{=} P_{x^n P_x} = P_{x^{n+2}}\,,$$

the last equality holding by power-associativity (Lemma 2.4). The rest follows by induction. □

In calculations, we will frequently use (3.4) without explicit reference.

Now assume Q is a uniquely 2-divisible, commutative A-loop. By (3.4), the twisted subgroup P_Q is also uniquely 2-divisible. Thus there is a natural Bruck loop operation $\circ$ on P_Q given by

$$P_x \circ P_y = (P_x P_y^2 P_x)^{1/2} \overset{(3.4)}{=} (P_x P_{y^2} P_x)^{1/2} \overset{(3.3)}{=} (P_{y^2 P_x})^{1/2} \overset{(3.4)}{=} P_{(y^2 P_x)^{1/2}}\,. \tag{3.5}$$

Thus as with uniquely 2-divisible Bol loops [8] or Moufang loops [10], we define a new binary operation (for which we will use the same symbol) on the underlying set Q by

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

By (3.5), the mapping $x \mapsto P_x$ is a surjective homomorphism from the magma $(Q, \circ)$ to the loop $(P_Q, \circ)$. In addition, note that this mapping is injective; indeed, if $P_x = \mathrm{id}\, Q$, then $x^2 = 1P_x = 1$ so that $x = 1$. Thus $(Q, \circ)$ is isomorphic to $(P_Q, \circ)$. Therefore we have most of the following.

Lemma 3.5. *For a uniquely 2-divisible, commutative A-loop Q, $(Q, \circ)$ is a Bruck loop. Powers in Q coincide with powers in $(Q, \circ)$.*

Proof. The remaining assertion about powers follows easily from (B), the power-associativity of Q (Lemma 2.4), and an easy induction argument. □

In the finite case, we may now reap the benefits of the known structure theory of Bruck loops of odd order [9] to obtain *Lagrange* and *Cauchy* theorems. We will implicitly use Lemma 3.1 in what follows.

Proposition 3.6. *Let $A \leq B$ be subloops of a finite commutative A-loop Q of odd order. Then $|A|$ divides $|B|$. In particular, the order of any element of Q divides $|Q|$.*

Proof. The subloops A and B of Q yield subloops $(A, \circ)$ and $(B, \circ)$ of $(Q, \circ)$. The result then follows from ([9], Corollary 4, p. 395). □

Proposition 3.7. *Let Q be a finite, commutative A-loop of odd order. If a prime p divides $|Q|$, then Q has an element of order p.*

Proof. This holds in the corresponding Bruck loop $(Q, \circ)$ [9]. Since powers of an element agree in both Q and $(Q, \circ)$, the result follows. □

Lemma 3.8. *Every inner mapping of a uniquely 2-divisible, commutative A-loop Q acts as an automorphism of $(Q, \circ)$.*

Proof. This is obvious from the definition of $\circ$. □

Lemma 3.9. *Let Q be a commutative A-loop of odd order. A subloop K of $(Q, \circ)$ is a subloop of Q if and only if $K\varphi = K$ for each $\varphi \in \mathrm{Inn}(Q) \cap \langle L_x : x \in K \rangle$.*

Proof. The "only if" direction is trivial, so assume the hypothesis of the converse. Fix $u, v \in K$. Note that $u^{-1}, v^{-1} \in K$, and since powers agree in $(Q, \circ)$ and Q, $v^{1/2} \in K$. Thus K also contains

$$(u \circ v^{1/2})^2 = vL_u L_{u^{-1}}^{-1} = vL_u^2 L_u^{-1} L_{u^{-1}}^{-1} = vL_u^2 L_{u^{-1},u}^{-1} .$$

By hypothesis, K then also contains vL_u^2. By induction, K contains vL_u^{2k} for all integers k. Now let $2n+1$ be the order of u. Then $L_u^{2n+1} \in \mathrm{Inn}(Q)$, since $1L_u^{2n+1} = u^{2n+1} = 1$. Hence K contains $vL_u^{-2n} L_u^{2n+1} = uv$, and also $vL_u^{2(-n-1)} L_u^{2n+1} = u \setminus v$. Thus K is closed under multiplication and left division in Q and is therefore a subloop of Q. □

At a particular point in the proof of Theorem 3.12 below, we will show that the Bruck loop associated to a certain commutative A-loop is commutative. In order to proceed, we will then need the corollary to the following technical lemma.

Lemma 3.10. *Let Q be a commutative A-loop and assume that the identity*

$$y^2 P_x = x^2 P_y \tag{3.6}$$

holds for all $x, y \in Q$. Then for all $x, y \in Q$,

$$y^2 P_x = x^2 y^2 . \tag{3.7}$$

Corollary 3.11. *Let Q be a uniquely 2-divisible, commutative A-loop. Then $(Q, \circ)$ is commutative if and only if $(Q, \circ)$ is isomorphic to Q.*

Indeed, in the uniquely 2-divisible case, (3.6) asserts that $(Q, \circ)$ is commutative, and (3.7) says that $(x \circ y)^2 = x^2 y^2$, that is, the squaring map $x \mapsto x^2$ is an isomorphism from $(Q, \circ)$ to Q.

Proof of Lemma 3.10. First we establish

$$(xy^2)P_x = xP_{xy} \tag{3.8}$$

for all $x, y \in Q$. Indeed, we have

$$\begin{aligned}(xy^2)P_x &\overset{(2.3)}{=} y^2P_xL_x \quad \overset{(3.6)}{=} x^2P_yL_x \quad \overset{(P)}{=} 1P_xP_yP_xL_{x^{-1}} \overset{(3.3)}{=} 1P_{yP_x}L_{x^{-1}}\\ &= x^{-1}\left(yP_x\right)^2 \overset{(3.1)}{=} xP_{x^{-1}\cdot yP_x} \overset{(P)}{=} xP_{xy}\,.\end{aligned}$$

Next, we will also require

$$x^{-1}P_{y^2} = y^2P_{x^{-1}}P_yL_x \tag{3.9}$$

for all $x, y \in Q$. For this, we compute

$$\begin{aligned}x^{-1}P_{y^2} &= x^{-1}P_{x\cdot x\setminus y^2} && \overset{(3.1)}{=} x(x\setminus y^2)^2\\ &= (x\setminus y^2)^2P_{y^{-1}}P_yL_x && \overset{(3.6)}{=} y^{-2}P_{x\setminus y^2}P_yL_x\\ &= \left((x\setminus y^2)\cdot(x\setminus y^2)^{-1}\setminus y^{-2}\right)P_yL_x && \overset{(AIP)}{=} \left((x\setminus y^2)\cdot(x^{-1}\setminus y^{-2})\setminus y^{-2}\right)P_yL_x\\ &= \left((x\setminus y^2)x^{-1}\right)P_yL_x && = y^2P_{x^{-1}}P_yL_x\,.\end{aligned}$$

Now, we compute

$$\begin{aligned}y^2P_xP_yL_x &\overset{(3.6)}{=} x^2P_y^2L_x && \overset{(P)}{=} 1P_xP_{y^2}P_xL_{x^{-1}}\\ &\overset{(3.3)}{=} 1P_{y^2P_x}L_{x^{-1}} && = x^{-1}\left(y^2P_x\right)^2\\ &\overset{(3.1)}{=} xP_{x^{-1}\cdot y^2P_x} && = xP_{xy^2}\\ &\overset{(AIP)}{=} xP_{x^{-1}y^{-1}}P_{xy}P_{xy^2} && \overset{(3.1)}{=} \left(x^{-1}y^{-2}\right)P_{xy}P_{xy^2}\\ &\overset{(AIP)}{=} (xy^2)^{-1}P_{xy^2\cdot(xy^2\setminus xy)}P_{xy^2} && \overset{(3.1)}{=} \left(xy^2\cdot(xy^2\setminus xy)^2\right)P_{xy^2}\\ &\overset{(3.8)}{=} (xy^2)P_{xy^2\cdot(xy^2\setminus xy)} && = (xy^2)P_{xy}\\ &\overset{(3.1)}{=} x^{-1}P_{xy}^2 && = x^{-1}P_{(xy)^2}\\ &\overset{(3.9)}{=} (xy)^2P_{x^{-1}}P_{xy}L_x\,.\end{aligned}$$

Canceling L_x, we have

$$y^2P_xP_y = (xy)^2P_{x^{-1}}P_{xy} = 1P_{xy}P_{x^{-1}}P_{xy} = 1P_{x^{-1}P_{xy}} \overset{(3.1)}{=} 1P_{xy^2} = (xy^2)^2\,.$$

Thus

$$y^2P_x = (xy^2)^2P_{y^{-1}} \overset{(3.6)}{=} y^{-2}P_{y^2x} \overset{(3.1)}{=} y^2x^2\,,$$

which is (3.7). □

We now turn to the main result of this section

Theorem 3.12 (Odd Order Theorem)**.** *Every commutative A-loop of odd order is solvable.*

Proof. Let Q be a minimal counterexample. Since normal subloops and quotients of commutative A-loops of odd order also have odd order, it follows that Q must be simple. Let N denote the derived subloop of $(Q, \circ)$, that is, the smallest normal subloop of $(Q, \circ)$ such that $(Q/N, \circ)$ is an abelian group. Finite Bruck loops of odd order are solvable ([10], Thm. 14(b)), and so N is a proper subloop. Clearly N is fixed by every automorphism of $(Q, \circ)$. By Lemma 3.8, N is fixed by every element of $\mathrm{Inn}(Q)$. Thus by Lemma 3.9, N is a subloop of Q itself. Since N is invariant under $\mathrm{Inn}(Q)$, N is normal in Q. But Q is simple, and so $N = \{1\}$. Therefore $(Q, \circ)$ is an abelian group. By Corollary 3.11, $(Q, \circ)$ is isomorphic to Q. Thus Q is an abelian group, which contradicts the assumption that Q is not solvable. □

4 Squares and an Associated Loop

In an abelian group, or even a commutative Moufang loop, the product of two squares is trivially a square, for in such loops the identity $x^2y^2 = (xy)^2$ holds. This identity does not hold in commutative A-loops. For example, there is a nonassociative, commutative A-loop of order 15 [7] in which the identity fails. Nevertheless, the more fundamental assertion about the product of two squares holds, as we are going to show.

Motivated by Theorem 4.1 below, we introduce a new binary operation in commutative A-loops:

$$x \diamond y = (xy \setminus x \cdot yx \setminus y)^{-1} = yL_{y,x} \cdot xL_{x,y}\,, \tag{$\diamond$}$$

where the second equality follows from (2.6) and (AIP).

Theorem 4.1. *For all x, y in a commutative A-loop,*

$$x^2y^2 = (x \diamond y)^2\,.$$

To establish the theorem, we require a couple of lemmas.

Lemma 4.2. *For all x, y in a commutative A-loop Q,*

$$x \diamond y = x^2 \cdot x \setminus (xy \setminus x)^{-1}\,. \tag{4.1}$$

Proof. First, we have

$$xL_{x,y} = (x^2y)L_{yx}^{-1} = yL_x^{-1}L_xL_{x^2}L_{yx}^{-1} \overset{(2.3)}{=} yL_x^{-1}L_{x^2}L_xL_{yx}^{-1} = yL_x^{-1}L_{x^2}L_y^{-1}L_{y,x}\,. \tag{4.2}$$

Thus,

$$\begin{aligned} x \diamond y \;&= yL_{y,x} \cdot xL_{x,y} && \overset{(4.2)}{=} yL_{y,x} \cdot yL_x^{-1}L_{x^2}L_y^{-1}L_{y,x} \\ &\overset{(A)}{=} [y \cdot yL_x^{-1}L_{x^2}L_y^{-1}]L_{y,x} && = yL_x^{-1}L_{x^2}L_{y,x} \\ &\overset{(2.1)}{=} yL_{y,x}L_x^{-1}L_{x^2} && \overset{(2.6)}{=} (xy \setminus x)^{-1}L_x^{-1}L_{x^2} \\ &= x^2 \cdot x \setminus (xy \setminus x)^{-1}\,, \end{aligned}$$

which gives (4.1). □

Lemma 4.3. *For all x, y in a commutative A-loop,*

$$x^{-1} \setminus (xy \setminus x) = y \setminus (yx \setminus y)^{-1}\,. \tag{4.3}$$

Proof. We compute

$$\begin{aligned} (y \setminus (yx \setminus y)^{-1})L_{x^{-1}}L_{xy} \;&= (yx \setminus y)^{-1}L_{x \setminus xy}^{-1}L_{x^{-1}}L_{xy} && \overset{(2.9)}{=} (yx \setminus y)^{-1}\,L_{x^{-1},xy} \\ &\overset{(A)}{=} \left((xy)L_{x^{-1},xy} \setminus yL_{x^{-1},xy}\right)^{-1} && \overset{(2.2)}{=} \left(xy \setminus yL_{x^{-1},xy}\right)^{-1} \\ &\overset{(2.8)}{=} \left(xy \setminus yL_{x,(xy)^{-1}}\right)^{-1} && = \left(xy \setminus (x(xy)^{-1})^{-1}\right)^{-1} \\ &\overset{(AIP)}{=} \left(xy \setminus (x^{-1} \cdot xy)\right)^{-1} && = x\,. \end{aligned}$$

Thus $y \setminus (yx \setminus y)^{-1} = xL_{xy}^{-1}L_{x^{-1}}^{-1} = x^{-1} \setminus (xy \setminus x)$, as claimed. □

Now we turn to the main result of this section.

Proof of Theorem 4.1. Set $z = x \diamond y$. Then

$$\begin{aligned} x^2 D_z &= z L_{x^2}^{-1} && \overset{(4.1)}{=} (x^2 \cdot x \setminus (xy \setminus x)^{-1}) L_{x^2}^{-1} \\ &= x \setminus (xy \setminus x)^{-1} && \overset{(AIP)}{=} (x^{-1} \setminus (xy \setminus x)) J \\ &\overset{(4.3)}{=} (y \setminus (yx \setminus y)^{-1}) J && = (y^2 \cdot y \setminus (yx \setminus y)^{-1}) L_{y^2}^{-1} J \\ &\overset{(4.1)}{=} z L_{y^2}^{-1} J && = y^2 D_z J \,. \end{aligned}$$

Thus $x^2 = x^2 D_z^2 = y^2 D_z J D_z \overset{(2.13)}{=} y^2 D_{z^2} = z^2 L_{y^2}^{-1}$, and so $x^2 y^2 = z^2$, as claimed. □

As the notation suggests, we will now consider $(Q, \diamond)$ as being a new magma constructed on a commutative A-loop Q. We introduce notation for the corresponding left translation map:

$$y S_x = x \diamond y \tag{S}$$

for all x, y. Note that

$$S_x = L_x D_x J L_x^{-1} L_{x^2} \tag{4.4}$$

by Lemma 4.2.

Proposition 4.4. *Let Q be a commutative A-loop and let $\diamond$ be defined by (⋄). Then $(Q, \diamond)$ is a power-associative, commutative loop with the same neutral element as Q. Powers in $(Q, \diamond)$ coincide with powers in Q.*

Proof. Commutativity is clear from the definition as is the fact that $(Q, \diamond)$ has the same neutral element as Q. By (4.4), each S_x is a permutation of Q. Hence $(Q, \diamond)$ is a loop. Finally, power-associativity of $(Q, \diamond)$ and the coinciding of powers follow from the power-associativity of Q (Lemma 2.4). □

For later use, we note the following.

Lemma 4.5. *For all x, y in a commutative A-loop Q and all $m, n \in \mathbb{Z}$,*

$$S_{x^n} L_{y, x^m} = L_{y, x^m} S_{x^n} \,. \tag{4.5}$$

Proof. This follows immediately from (4.4), (2.4), (2.5) and (AIP). □

We conclude this section by noting that for uniquely 2-divisible, commutative A-loops, the loop operation $\diamond$ gives nothing new.

Lemma 4.6. *If Q is a uniquely 2-divisible, commutative A-loop, then $(Q, \diamond)$ is isomorphic to Q.*

Proof. Indeed, the conclusion of Theorem 4.1 shows that the squaring map is an isomorphism from $(Q, \diamond)$ to Q. □

We will return to the associated loop operation $(Q, \diamond)$ in §6 when we consider commutative A-loops of exponent 2.

5 The Decomposition Theorem

Our main goal in this section is the following.

Theorem 5.1 (Decomposition for Finite Commutative A-loops)**.** *If Q is a finite commutative A-loop, then $Q = K(Q) \times H(Q)$, where $K(Q) = \{x \in Q \,|\, |x| \text{ is odd }\}$ and $H(Q) = \{x \in Q \,|\, x^{2^n} = 1 \text{ for some } n \in \mathbb{Z}\}$.*

In addition, $K(Q)$ has odd order (Theorem 5.3(v) below), and we will show later that $H(Q)$ has order a power of 2 (Theorem 7.1).

Proposition 5.2. *In a commutative A-loop Q, the set $K_1(Q) = \{x^2 \,|\, x \in Q\}$ is a normal subloop of Q.*

Proof. The set K_1 is closed under multiplication by Theorem 4.1. By Proposition 4.4, given $x, z \in Q$, there exists a unique $y \in Q$ such that $x \diamond y = z$, and so $x^2y^2 = z^2$ by Theorem 4.1 once more. Thus K_1 is a subloop of Q. The normality of K_1 follows from the fact that all inner mappings of Q are automorphisms of Q and hence preserve squares. □

Theorem 5.3. *Let Q be a commutative A-loop. For $n \geq 1$, define*

$$K_n(Q) = \{x^{2^n} \mid x \in Q\},$$
$$K(Q) = \bigcap_{n \geq 1} K_n(Q).$$

Then:

- *i)* $K_{n+1}(Q) = \{x^2 \mid x \in K_n(Q)\}$ *for every* $n \geq 0$.
- *ii)* $K_{n+1}(Q) \subseteq K_n(Q)$ *for every* $n \geq 0$.
- *iii)* $K_n(Q) \trianglelefteq Q$ *for every* $n \geq 0$.
- *iv)* $K(Q) \trianglelefteq Q$.
- *v) If Q is finite, then $K(Q) = \{x \in Q \mid |x|$ is odd $\}$ and $|K(Q)|$ is odd.*

Proof. If $x \in K_n(Q)$ then $x = y^{2^n}$ for some $y \in Q$ and $x^2 = y^{2^{n+1}} \in K_{n+1}(Q)$. Conversely, if $x \in K_{n+1}(Q)$ then $x = z^{2^{n+1}} = (z^{2^n})^2$ for some $z \in Q$ and $z^{2^n} \in K_n(Q)$. This proves (i) and (ii).

By Proposition 5.2, $K_1(Q) \leq Q$. Assume that $K_n(Q) \leq Q$. By (i), Proposition 5.2 applied to $K_n(Q)$ yields $K_{n+1}(Q) \leq K_n(Q) \leq Q$. The normality of $K_n(Q)$ in the A-loop Q follows for free. This proves (iii) and (iv).

For (v), assume that Q is finite. Then there is n such that $K_{n+1}(Q) = K_n(Q) = K(Q) = \{x^2 \mid x \in K(Q)\}$, by (i). The mapping $x \mapsto x^2$ is a bijection of $K(Q)$ fixing $1 \in K(Q)$, so $K(Q)$ contains no elements of order 2 and hence no elements of even order. Conversely, pick $x \in Q$ of odd order, say $|x| = 2m + 1$. The equality $x = x^{2m+2} = (x^{m+1})^2$ then implies $x \in K_1(Q)$, so that $x^{m+1} \in K_1(Q)$ by (iii). Thus $x \in K_2(Q)$ by (i), and so on, proving $x \in K(Q)$. The remaining assertion follows from Lemma 3.1. □

Lemma 5.4. *For every x, y in a commutative A-loop Q,*

$$(x \setminus (y \setminus x))^2 \setminus (y^{-1}(y \setminus x))^2 = (x \setminus y)^{-2} \tag{5.1}$$

Proof. With y replaced by $x \setminus y$, (2.7) yields

$$x(x \setminus y)^2 = y(y \setminus x)^{-1}. \tag{5.2}$$

Replacing y with $y \setminus x$ and using $(y \setminus x) \setminus x = y$ gives

$$x(x \setminus (y \setminus x))^2 = y^{-1}(y \setminus x). \tag{5.3}$$

Applying J and using (AIP) gives

$$x^{-1}(x \setminus (y \setminus x))^{-2} = y(y \setminus x)^{-1}. \tag{5.4}$$

Putting (5.2) and (5.4) together, we have

$$(x \setminus y)^2(x \setminus (y \setminus x))^{-2} = xD_{y(y \setminus x)^{-1}} \cdot x^{-1}D_{y(y \setminus x)^{-1}} \overset{(2.14)}{=} (y(y \setminus x)^{-1})^2.$$

Applying J to both sides and using (AIP), we have $(x \setminus y)^{-2}(x \setminus (y \setminus x))^2 = (y^{-1}(y \setminus x))^2$, and this is clearly equivalent to (5.1). □

Proposition 5.5. *Let Q be a commutative A-loop, and let $x \in Q$ satisfy $x^{2^n} = 1$. Then $(xy)^{2^n} = y^{2^n}$ for every $y \in Q$.*

Proof. We proceed by induction on n. The claim is clearly true when $n = 0$. Let $n \geq 0$, assume that the claim holds for n, and let $x \in Q$ satisfy $x^{2^{n+1}} = 1$. Then the induction assumption yields

$$(x^2 y)^{2^n} = y^{2^n} = (x^2(x^2 \setminus y))^{2^n} = (x^2 \setminus y)^{2^n} \tag{5.5}$$

for every $y \in Q$. We may apply any automorphism φ to (5.5), and then set $z = y\varphi$ to obtain $((x\varphi)^2 z)^{2^n} = z^{2^n} = ((x\varphi)^2 \setminus z)^{2^n}$ for all $z \in Q$. In particular, we choose $\varphi = JL_{x,x\setminus y}$ (by (A) and (AIP)). Then $xJL_{x,x\setminus y} = y \setminus (x \setminus y)$ by (2.6) (or direct calculation). Hence

$$(z(y \setminus (x \setminus y))^2)^{2^n} = z^{2^n} = ((y \setminus (x \setminus y))^2 \setminus z)^{2^n} \tag{5.6}$$

for every $y, z \in Q$. Thus

$$\begin{aligned} y^{2^{n+1}} &\overset{(5.6)}{=} [y(y \setminus (x \setminus y))^2]^{2^{n+1}} \overset{(5.3)}{=} [x^{-1}(x \setminus y)]^{2^{n+1}} = [(x^{-1}(x \setminus y))^2]^{2^n} \\ &\overset{(5.6)}{=} [(y \setminus (x \setminus y))^2 \setminus (x^{-1}(x \setminus y))^2]^{2^n} \overset{(5.1)}{=} (y \setminus x)^{-2^{n+1}} . \end{aligned}$$

Then

$$\begin{aligned} (y^{-1})^{-2^{n+1}} = y^{2^{n+1}} &\overset{(2.2)}{=} y^{2^{n+1}} L_{y,y^{-1}} = (y \setminus x)^{-2^{n+1}} L_{y,y^{-1}} \\ &\overset{(A)}{=} ((y \setminus x) L_{y,y^{-1}})^{-2^{n+1}} = (y^{-1}x)^{-2^{n+1}} . \end{aligned}$$

Taking inverses and replacing y with y^{-1}, we obtain $y^{2^{n+1}} = (xy)^{2^{n+1}}$, which completes the proof. □

Theorem 5.6. *Let Q be a commutative A-loop. For $n \geq 0$, let*

$$\begin{aligned} H_n(Q) &= \{x \in Q \mid x^{2^n} = 1\}, \\ H(Q) &= \bigcup_{n \geq 0} H_n(Q). \end{aligned}$$

Then:

i) $H_{n+1}(Q) = \{x \in Q \mid x^2 \in H_n(Q)\}$ *for every* $n \geq 0$.

ii) $H_{n+1}(Q) \supseteq H_n(Q)$ *for every* $n \geq 0$.

iii) $H_n(Q) \trianglelefteq Q$ *for every* $n \geq 0$.

iv) $H(Q) \trianglelefteq Q$.

Proof. Parts (i) and (ii) are obvious. For (iii) and (iv), it suffices to show that $H_n(Q) \leq Q$ for every $n \geq 0$ and $H(Q) \leq Q$. Let $x \in H_n(Q)$, $y \in H_m(Q)$ and let $k = \max\{n, m\}$. Then Proposition 5.5 yields $(xy)^{2^k} = x^{2^k} = 1$ and $(x \setminus y)^{2^k} = (x \cdot x \setminus y)^{2^k} = y^{2^k} = 1$. □

Finally, we turn to the proof of the main result of this section.

Proof of Theorem 5.1. By Theorems 5.3 and 5.6, K and H are normal subloops of Q. Clearly $K \cap H = 1$, and $KH = Q$ is proved in the same way as for groups (since the argument takes place in cyclic subgroups, by power-associativity). Then $Q = K \times H$ follows. □

6 Commutative A-loops of exponent 2

We now turn to commutative A-loops of exponent 2. The following result shows why this special case is of particular importance.

Proposition 6.1. *A finite simple commutative A-loop is either a cyclic group of order p for some odd prime p, or it has exponent 2.*

Proof. Let Q be a finite simple commutative A-loop. By the Decomposition Theorem 5.1, $Q = K(Q) \times H(Q)$. Since Q is simple, $Q = K(Q)$ or $Q = H(Q)$. In the former case, Q is solvable by Theorems 5.3(v) and 3.12. Thus Q is both simple and solvable, and hence is a cyclic group of odd prime order. Now assume $Q = H(Q)$, that is, every element of Q has order a power of 2. The subloop $K_1(Q) = \{x^2 \mid x \in Q\}$ is normal (Proposition 5.2), and so either $K_1(Q) = Q$ or $K_1(Q) = \langle 1 \rangle$. In the former case, the squaring map is a bijection by finiteness, but then Q has odd order by Lemma 3.1, a contradiction. Thus for every $x \in Q$, $x^2 = 1$, that is, Q has exponent 2. □

Our goal in this section is to establish the following.

Theorem 6.2. *Let Q be a commutative A-loop of exponent 2. Then $(Q, \diamond)$ is an elementary abelian 2-group.*

Corollary 6.3. *If Q is a finite, commutative A-loop of exponent 2, then $|Q|$ is a power of 2.*

The proof of Theorem 6.2 will require some technical lemmas. *Throughout the rest of this section*, let Q be a commutative A-loop of exponent 2. The operation $\diamond$ and the corresponding translations S_x simplify accordingly:

$$x \diamond y = x \setminus (xy \setminus x)$$
$$S_x = L_x D_x L_x^{-1}$$

Thus $S_x^2 = L_x D_x L_x^{-1} L_x D_x L_x^{-1} = L_x D_x^2 L_x^{-1} = \mathrm{id}\, Q$. This establishes the following.

Lemma 6.4. *For all $x, y \in Q$, $x \diamond (x \diamond y) = y$, that is, $S_x^2 = \mathrm{id}\, Q$.*

Lemma 6.5. *For all $x \in Q$,*

$$S_x = L_x D_x L_x^{-1} = L_x^{-1} D_x L_x \,. \tag{6.1}$$

Proof. The first equality has already been established. Since Q has exponent 2, $D_x = D_{xL_x^2}$ for each x. Now $L_x^2 = L_{x,x} \in \mathrm{Inn}(Q)$, and so we have $L_x^2 D_x = L_x^2 D_{xL_x^2} \overset{(A)}{=} D_x L_x^2$. Applying L_x^{-1} on the left and on the right, we obtain the desired result. □

Lemma 6.6. *For all $x, y, z \in Q$,*

$$y L_{z \setminus (x \cdot zy), z} S_{zy} = z L_y L_x^{-1} D_y L_x \,. \tag{6.2}$$

Proof. First, we compute

$$\begin{aligned} y L_{x,z} S_{zy} L_{zx \setminus zy}^{-1} L_{zx} &= y L_{x,z} S_{zy} L_{zy}^{-1} [L_{zy} L_{zx \setminus zy}^{-1} L_{zx}] && \overset{(2.10)}{=} y L_{x,z} S_{zy} [L_{zy}^{-1} L_{zx,zy}] \\ &\overset{(2.4)}{=} y L_{x,z} [S_{zy} L_{zx,zy}] L_{zy}^{-1} && \overset{(4.5)}{=} y [L_{x,z} L_{zx,zy}] S_{zy} L_{zy}^{-1} \\ &= [yL_x] L_z [L_{zx}^{-1} L_{zx}] L_{zy} L_{zy \cdot zx}^{-1} S_{zy} L_{zy}^{-1} && = x L_y L_z L_{zy} L_{zy \cdot zx}^{-1} [S_{zy} L_{zy}^{-1}] \\ &\overset{(6.1)}{=} x L_y L_z L_{zy} L_{zy \cdot zx}^{-1} L_{zy}^{-1} D_{zy} \,. \end{aligned}$$

Now since Q has exponent 2, $1 L_y L_z L_{zy} = 1$, and so $L_y L_z L_{zy} \in \mathrm{Inn}(Q)$. Also, $zx \cdot zy = (y \setminus x) L_y L_z L_{zy}$. Thus we may apply (A) to get

$$\begin{aligned} y L_{x,z} S_{zy} L_{zx \setminus zy}^{-1} L_{zx} &= x L_{y \setminus x}^{-1} L_y L_z [L_{zy} L_{zy}^{-1}] D_{zy} = [x L_{y \setminus x}^{-1}] L_y L_z D_{zy} \\ &= [y D_x^2 L_y L_z] D_{zy} && = z D_{zy} \\ &= y \,. \end{aligned}$$

where we have used $y^2 = 1$ in the penultimate step. Hence

$$yL_{x,z}S_{zy} = yL_{zx}^{-1}L_{zx\setminus zy} \overset{(2.12)}{=} yL^{-1}_{(zy\setminus zx)\setminus zy}L_{zy\setminus zx}\,.$$

Replacing x with $xL_{zy}L_z^{-1} = z\setminus(x\cdot zy)$, we obtain

$$yL_{z\setminus(x\cdot zy),z}S_{zy} = yL^{-1}_{x\setminus zy}L_x = zL_yL_x^{-1}D_yL_x\,.$$

This establishes (6.2). □

Lemma 6.7. *For all $u,v,w\in Q$,*

$$uL_{v\setminus(w\cdot uv),v} = uL_vL_w^{-1}D_vL_w\,. \tag{6.3}$$

Proof. We compute

$$\begin{aligned}
uL_{v\setminus(w\cdot uv),v} &= [uL_{v\setminus(w\cdot uv)}]L_vL_{w\cdot uv}^{-1} &&= w[L_{uv}L_v^{-1}L_u]L_vL_{w\cdot uv}^{-1}\\
&\overset{(2.10)}{=} wL_{u,uv}L_vL_{w\cdot uv}^{-1} &&= wL_{v\setminus uv,uv}L_vL_{w\cdot uv}^{-1}\\
&\overset{(2.11)}{=} w[L_{uv\setminus v,uv}L_v]L_{w\cdot uv}^{-1} &&= [wL_{uv\setminus v}]L_{uv}L_{w\cdot uv}^{-1}\\
&= (uv\setminus v)L_wL_{uv}L_{w\cdot uv}^{-1} &&= vL_{uv}^{-1}L_{w,uv}\\
&\overset{(2.10)}{=} vL^{-1}_{w\setminus uv}L_w &&= uL_vL_w^{-1}D_vL_w\,,
\end{aligned}$$

which establishes (6.3). □

Lemma 6.8. *For all $u,v,w\in Q$,*

$$uL^{-1}_{v\setminus w}L_vL_{vw,u} = wu\,. \tag{6.4}$$

Proof. We compute

$$\begin{aligned}
u[L^{-1}_{v\setminus w}L_v]L_{vw,u} &\overset{(2.9)}{=} uL_{v,w}L_w^{-1}L_{vw,u} &&\overset{(2.4)}{=} uL_w^{-1}[L_{v,w}L_{vw,u}]\\
&= [uL_w^{-1}L_v]L_wL_uL_{vw\cdot u}^{-1} &&= vL_{w\setminus u}L_wL_uL_{vw\cdot u}^{-1}\\
&= v[L_{w\setminus u}L_{w,u}]L_{wu}L_{vw\cdot u}^{-1} &&\overset{(2.9)}{=} vL_wL_uL_{wu}L_{vw\cdot u}^{-1}\\
&= ((u\cdot vw)\cdot wu)L_{vw\cdot u}^{-1} &&= wu\,,
\end{aligned}$$

which establishes (6.4). □

Lemma 6.9. *For all $u,v,w\in Q$,*

$$vL_{w,u}S_{uv} = vL_{w,u}L_u^{-1}L_v\,. \tag{6.5}$$

Proof. We begin with

$$vL_{u\setminus(w\cdot uv),u}S_{uv} \overset{(6.2)}{=} uL_vL_w^{-1}D_vL_w \overset{(6.3)}{=} uL_{v\setminus(w\cdot vu),v}\,.$$

Replacing w with $wL_{uv}^{-1}L_u$, we have

$$\begin{aligned}
vL_{w,u}S_{uv} &= uL_{v\setminus uw,v} &&\overset{(2.11)}{=} uL_{uw\setminus v,v}\\
&\overset{(2.9)}{=} uL^{-1}_{(uw\setminus v)\setminus v}L_{uw\setminus v}L_v &&= uL_{uw}^{-1}L_{uw\setminus v}L_v\\
&= vL_{uw}^{-1}L_{uw\setminus u}L_v &&\overset{(2.12)}{=} vL^{-1}_{(u\setminus uw)\setminus u}L_{u\setminus uw}L_v\\
&= vL^{-1}_{w\setminus u}L_wL_v &&\overset{(2.9)}{=} vL_{w,u}L_u^{-1}L_v\,.
\end{aligned}$$

This establishes (6.5). □

Lemma 6.10. *For all $x, y \in Q$,*

$$L_x^{-1} D_y L_x = L_y^{-1} D_x L_y D_{xy} \,. \tag{6.6}$$

Proof. We have

$$\begin{aligned} zL_yL_x^{-1}D_yL_x &\overset{(6.2)}{=} yL_{z\setminus(x\cdot zy)}S_{zy} && \overset{(6.3)}{=} y[L_zL_x^{-1}]D_zL_xS_{zy} \\ &= yL_{z\setminus x}^{-1}[L_{z\setminus x,z}D_z]L_xS_{zy} && \overset{(2.5)}{=} yL_{z\setminus x}^{-1}D_z[L_{z\setminus x,z}L_x]S_{zy} \\ &= yL_{z\setminus x}^{-1}D_zL_{z\setminus x}L_zS_{zy}\,. \end{aligned}$$

Now set $u = yL_{z\setminus x}^{-1}D_zL_{z\setminus x} = zL_{(z\setminus x)\setminus y}^{-1}L_{z\setminus x}$, and observe that

$$uL_{(z\setminus x)y,z} \overset{(6.4)}{=} yz\,. \tag{6.7}$$

Thus using the commutativity of $\diamond$, we compute

$$\begin{aligned} zL_yL_x^{-1}D_yL_x &= (zu)S_{zy} && = (zy)S_{zu} && \overset{(6.7)}{=} uL_{(z\setminus x)y,z}S_{zu} \\ &\overset{(6.5)}{=} uL_{(z\setminus x)y,z}L_z^{-1}L_u && \overset{(6.7)}{=} (yz)L_z^{-1}L_u && = yL_u \\ &= uL_y && = zL_{(z\setminus x)\setminus y}^{-1}L_{z\setminus x}L_y && \overset{(2.9)}{=} zL_{z\setminus x,y} \\ &= zL_{z\setminus x}L_yL_{(z\setminus x)y}^{-1} && = (yx)L_{(z\setminus x)y}^{-1} && = zD_xL_yD_{xy}\,. \end{aligned}$$

Thus $L_yL_x^{-1}D_yL_x = D_xL_yD_{xy}$. Multiplying on the left by L_y^{-1}, we obtain (6.6). □

Lemma 6.11. *For all $x, y \in Q$,*

$$L_x^{-1} D_y L_x = L_{xy}^{-1} S_{(xy)\setminus x} L_{xy}\,. \tag{6.8}$$

Proof. We compute

$$\begin{aligned} L_x^{-1}D_yL_x &= L_x^{-1}L_y^{-1}S_yL_yL_x && = L_x^{-1}L_y^{-1}S_yL_{y,x}L_{xy} \\ &\overset{(A)}{=} L_x^{-1}L_y^{-1}L_{y,x}S_{yL_{y,x}}L_{xy} && \overset{(2.6)}{=} L_{xy}^{-1}S_{(xy)\setminus x}L_{xy}\,, \end{aligned}$$

where we have also used the assumption that Q has exponent 2 in the last step. □

Finally, we have enough for the main result of this section.

Proof of Theorem 6.2. By commutativity of $\diamond$ (Proposition 4.4) and $x \diamond x = x^2 = 1$ for all $x \in Q$, all that is needed is to show that $\diamond$ is associative. First, apply (6.8) to both sides of (6.6) to obtain $L_{xy}^{-1}S_{(xy)\setminus x}L_{xy} = L_{yx}^{-1}S_{(yx)\setminus y}L_{yx}D_{xy}$, or $S_{(xy)\setminus x} = S_{(yx)\setminus y}L_{yx}D_{xy}L_{xy}^{-1} = S_{(yx)\setminus y}S_{xy}$. Replace x with $y \setminus x$ to get $S_{x\setminus(y\setminus x)} = S_{x\setminus y}S_x$. Replace y with xy to obtain $S_{x\setminus(xy\setminus x)} = S_yS_x$, or $S_{x\diamond y} = S_yS_x$. This is precisely associativity of $\diamond$: applying both sides to z, we have $(x \diamond y) \diamond z = x \diamond (y \diamond z)$ for all $x, y, z \in Q$. This completes the proof. □

7 p-loops

For a finite, power-associative loop Q, there are at least two reasonable ways to define what it means for Q to be a *p-loop*: either every element of Q has order a power of p, or $|Q|$ is a power of p. Fortunately, these two notions are equivalent for groups, Moufang loops, and, as we are about to show, for commutative A-loops.

Theorem 7.1. *Let Q be a finite commutative A-loop and let p be a prime. Then $|Q|$ is a power of p if and only if every element of Q has order a power of p.*

Proof. Assume first that p is odd. If $|Q|$ is a power of p, then by Proposition 3.6, every element of Q has order a power of p. Conversely, if $|Q|$ is divisible by an odd prime q, then by Proposition 3.7(iii), Q contains an element of order q. Thus if every element of Q has order a power of p, $|Q|$ must be a power of p.

Now assume that $p = 2$ and that $|Q|$ is a power of 2. Since $Q = K(Q) \times H(Q)$ (Theorem 5.1) and $|K(Q)|$ is odd (Theorem 5.3), we must have $K(Q) = \langle 1 \rangle$, and so $Q = K(Q)$, that is, every element of Q has order a power of 2.

For the converse, assume that Q is a smallest commutative A-loop of exponent a power of 2 such that $|Q|$ is not a power of 2. Consider the normal subloop $1 < H_1 = \{x \in Q \,|\, x^2 = 1\}$, *cf.* Theorem 5.6. Then $|H_1|$ is a power of 2 by Corollary 6.3. If $H_1 = Q$, we have reached a contradiction. If $H_1 < Q$ then $|Q/H_1|$ is a power of 2 by minimality, and so $|Q| = |H_1| \cdot |Q/H_1|$ is a power of 2, a contradiction. □

Unlike in the case of abelian groups, for a finite commutative A-loop Q, the normal subloop $K(Q)$ does not necessarily decompose as a direct product of p-loops. For example, Drápal [7] constructed a commutative A-loop of order 15 that is not a direct product of a 3-loop and a 5-loop.

Theorem 7.2 (Lagrange and Cauchy Theorems)**.** *Let Q be a finite commutative A-loop. Then:*

i) *If $x \in A \leq Q$ then both $|x|$ and $|A|$ divide $|Q|$.*

ii) *If a prime p divides $|Q|$ then Q has an element of order p.*

Proof. Combine Theorems 5.1, 7.1 and Propositions 3.6, 3.7. □

8 Open Problems

We conclude this paper with some open problems.

Problem 8.1. *Does there exist a nonassociative, finite simple commutative A-loop?*

By Proposition 6.1 and Corollary 6.3, such a loop would have exponent 2 and order a power of 2. To get some insight into the problem, more constructions of commutative A-loops which are 2-loops are needed; see [11].

Recall that the *center* of a loop Q is the set of all elements a satisfying $a \cdot xy = x \cdot ay = xa \cdot y$ for all x, y. In groups and Moufang loops, the center of a p-loop is always nontrivial, and thus such loops are centrally nilpotent.

Problem 8.2. *Let p be an odd prime. Does there exist a finite commutative A-loop of order a power of p with trivial center?*

By a classic result of Albert [1], it would be sufficient to show that $\mathrm{Mlt}(Q)$ is a p-group.

The restriction to odd p is necessary. There exist commutative A-loops of exponent 2 of all orders 2^n, $n \geq 4$ with trivial center [11].

For a set π of primes, a positive integer n is a *π-number* if $n = 1$ or if n is a product of primes in π. For each positive integer n, let n_π denote the largest π-number dividing n. A subloop K of a finite, power-associative loop Q is a *Hall π-subloop* if $|K| = |Q|_\pi$. In case $\pi = \{p\}$, we say that K is a *Sylow p-subloop* of Q.

Problem 8.3. *Let Q be a commutative A-loop.*

i) *For each set π of primes, does Q have a Hall π-subloop?*

ii) *For each prime p, does Q have a Sylow p-subloop?*

Sylow 2-subloops certainly exist by Theorems 5.1 and 7.1. In both the Hall and Sylow cases, the problem reduces to considering commutative A-loops of odd order. Hall and Sylow subloops of the associated Bruck loop $(Q, \circ)$ exist [9], so the question is whether or not these are also subloops of Q itself.

References

[1] A. A. Albert, Quasigroups II, *Trans. Amer. Math. Soc.* **55** (1944), 401–419.

[2] M. Aschbacher, *Finite Group Theory*, Cambridge Univ. Press, Cambridge, 1986.

[3] M. Aschbacher, Near subgroups of finite groups, *J. Group Theory* **1** (1998), 113–129.

[4] V. D. Belousov, *Foundations of the Theory of Quasigroups and Loops*, Izdat. Nauka, Moscow, 1967 (Russian).

[5] R. H. Bruck, *A Survey of Binary Systems*, Springer-Verlag, 1971.

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

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

[8] T. Foguel, M. K. Kinyon, and J. D. Phillips, On twisted subgroups and Bol loops of odd order, *Rocky Mountain J. Math* **36** (2006), 183–212.

[9] G. Glauberman, On loops of odd order I, *J. Algebra* **1** (1964), 374–396.

[10] G. Glauberman, On loops of odd order II, *J. Algebra* **8** (1968), 393–414.

[11] P. Jedlička, M. K. Kinyon and P. Vojtěchovský, Commutative A-loops: constructions and classification, *Comm. Algebra*, Commun. in Alg. **38**, 9 (2010), 3243–3267

[12] T. Kepka, M. K. Kinyon and J. D. Phillips, The structure of F-quasigroups, *J. Algebra* **317** (2007), 435–461.

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

[14] M. K. Kinyon, K. Kunen and J. D. Phillips, A generalization of Moufang loops and A-loops, in preparation.

[15] W. McCune, *Prover9*, version 2008-06A, (`http://www.cs.unm.edu/ mccune/prover9/`)

[16] J. M. Osborn, A theorem on *A*-loops, *Proc. Amer. Math. Soc.* **9** (1958), 347–349.

[17] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math. **8**, Heldermann Verlag, Berlin, 1990.

[18] P. Plaumann and L. Sabinina, On nuclearly nilpotent loops of finite exponent, *Comm. Alg.* **36** (2008), 1346–1353.

4 Nilpotency in automorphic loops of prime power order

Přemysl Jedlička, Michael K. Kinyon, Petr Vojtěchovský

Abstract

A loop is automorphic if its inner mappings are automorphisms. Using so-called associated operations, we show that every commutative automorphic loop of odd prime power order is centrally nilpotent. Starting with anisotropic planes in the vector space of 2×2 matrices over the field of prime order p, we construct a family of automorphic loops of order p^3 with trivial center.

1 Introduction

A classical result of group theory is that p-groups are (centrally) nilpotent. The analogous result does not hold for loops.

The first difficulty is with the concept of a p-loop. For a prime p, a finite group has order a power of p if and only if each of its elements has order a power of p, so p-groups can be defined in two equivalent ways. Not so for loops, where the order of an element might not be well defined, and even if it is, the two natural p-loop concepts might not be equivalent.

However, there exist several varieties of loops where the analogy with group theory is complete. For instance, a Moufang loop has order a power of p if and only if each of its elements has order a power of p, and, moreover, every Moufang p-loop is nilpotent [7, 8].

We showed in [10, Thm. 7.1] that a finite commutative automorphic loop has order a power of p if and only if each of its elements has order a power of p. The same is true for automorphic loops, by [13], *provided* that p is odd; the case $p = 2$ remains open.

In this paper we study nilpotency in automorphic loops of prime power order. We prove:

Theorem 1.1. *Let p be an odd prime and let Q be a finite commutative automorphic p-loop. Then Q is centrally nilpotent.*

Since there is a (unique) commutative automorphic loop of order 2^3 with trivial center, cf. [9], Theorem 1.1 is best possible in the variety of commutative automorphic loops. (The situation for $p = 2$ is indeed complicated in commutative automorphic loops. By [9, Prop. 6.1], if a nonassociative finite simple commutative automorphic loop exists, it has exponent two. We now know that no nonassociative finite simple commutative automorphic loop of order less than 2^{12} exists [11].)

In fact, Theorem 1.1 is best possible even in the variety of automorphic loops, because for every prime p we construct here a family of automorphic loops of order p^3 with trivial center.

1.1 Background

A *loop* $(Q, \cdot)$ is a set Q with a binary operation $\cdot$ such that (i) for each $x \in Q$, the *left translation* $L_x : Q \to Q; y \mapsto yL_x = xy$ and the *right translation* $R_x : Q \to Q; y \mapsto yR_x = yx$ are bijections, and (ii) there exists $1 \in Q$ satisfying $1 \cdot x = x \cdot 1 = x$ for all $x \in Q$.

The left and right translations generate the *multiplication group* $\operatorname{Mlt} Q = \langle L_x, R_x \mid x \in Q \rangle$. The *inner mapping group* $\operatorname{Inn} Q = (\operatorname{Mlt} Q)_1$ is the stabilizer of $1 \in Q$. Standard references for the theory of loops are [1, 2, 18].

A loop Q is *automorphic* (or sometimes just an *A-loop*) if every inner mapping of Q is an automorphism of Q, that is, $\operatorname{Inn} Q \leq \operatorname{Aut} Q$.

The study of automorphic loops was initiated by Bruck and Paige [3]. They obtained many basic results, not the least of which is that automorphic loops are *power-associative*, that is, for all x and

all integers m, n, $x^m x^n = x^{m+n}$. In power-associative loops, the *order* of an element may be defined unambiguously.

For commutative automorphic loops, there now exists a detailed structure theory [9], as well as constructions and small order classification results [10].

Informally, the *center* $Z(Q)$ of a loop Q is the set of all elements of Q which commute and associate with all other elements. It can be characterized as $Z(Q) = \mathrm{Fix}(\mathrm{Inn}(Q))$, the set of fixed points of the inner mapping group. (See §2 for the more traditional definition.)

The center is a *normal* subloop of Q, that is, $Z(Q)\varphi = Z(Q)$ for every $\varphi \in \mathrm{Inn}\, Q$. Define $Z_0(Q) = \{1\}$, and $Z_{i+1}(Q)$, $i \geq 0$, as the preimage of $Z(Q/Z_i(Q))$ under the canonical projection. This defines the *upper central series*

$$1 \leq Z_1(Q) \leq Z_2(Q) \leq \cdots \leq Z_n(Q) \leq \cdots \leq Q$$

of Q. If for some n we have $Z_{n-1}(Q) < Z_n(Q) = Q$ then Q is said to be *(centrally) nilpotent of class n*.

1.2 Summary

The proof of our main result, Theorem 1.1, is based on a construction from [9]. On each commutative automorphic loop $(Q, \cdot)$ which is uniquely 2-divisible (*i.e.*, the squaring map $x \mapsto x \cdot x$ is a permutation), there exists a second loop operation $\circ$ such that $(Q, \circ)$ is a Bruck loop (see §3), and such that powers of elements in $(Q, \cdot)$ coincide with those in $(Q, \circ)$.

Glauberman [6] showed that for each odd prime p a finite Bruck p-loop is centrally nilpotent. Theorem 1.1 will therefore follow immediately from this and from the following result:

Theorem 1.2. *Let $(Q, \cdot)$ be a uniquely 2-divisible commutative automorphic loop with associated Bruck loop $(Q, \circ)$. Then $Z_n(Q, \circ) = Z_n(Q, \cdot)$ for every $n \geq 0$.*

After reviewing preliminary results in §2, we discuss the associated Bruck loop in §3 and prove Theorem 1.2 in §4.

In §5, we use anisotropic planes in the vector space of 2×2 matrices over $GF(p)$ to obtain automorphic loops of order p^3 with trivial center. We obtain one such loop for $p = 2$ (this turns out to be the unique commutative automorphic loop of order 2^3 with trivial center), two such loops for $p = 3$, three such loops for $p \geq 5$, and at least one (conjecturally, three) such loop for every prime $p \geq 7$

Finally, we pose open problems in §6.

2 Preliminaries

In a loop $(Q, \cdot)$, there are various subsets of interest:

- the *left nucleus* $N_\lambda(Q) = \{a \in Q \mid ax \cdot y = a \cdot xy,\ \forall x, y \in Q\}$
- the *middle nucleus* $N_\mu(Q) = \{a \in Q \mid xa \cdot y = x \cdot ay,\ \forall x, y \in Q\}$
- the *right nucleus* $N_\rho(Q) = \{a \in Q \mid xy \cdot a = x \cdot ya,\ \forall x, y \in Q\}$
- the *nucleus* $N(Q) = N_\lambda(Q) \cap N_\mu(Q) \cap N_\rho(Q)$
- the *commutant* $C(Q) = \{a \in Q \mid ax = xa,\ \forall x \in Q\}$
- the *center* $Z(Q) = N(Q) \cap C(Q)$.

The commutant is not necessarily a subloop, but the nuclei are.

Proposition 2.1. *[3] In an automorphic loop $(Q, \cdot)$, $N_\lambda(Q) = N_\rho(Q) \leq N_\mu(Q)$. If, in addition, $(Q, \cdot)$ is commutative, $Z(Q) = N_\lambda(Q)$.*

We will also need the following (well known) characterization of $C(Q) \cap N_\rho(Q)$:

Lemma 2.2. *Let $(Q, \cdot)$ be a loop. Then $a \in C(Q) \cap N_\rho(Q)$ if and only if $L_a L_x = L_x L_a$ for all $x \in Q$.*

Proof. If $a \in C(Q) \cap N_\rho(Q)$, then for all $x, y \in Q$, $a \cdot xy = xy \cdot a = x \cdot ya = x \cdot ay$, that is, $L_a L_x = L_x L_a$. Conversely, if $L_a L_x = L_x L_a$ holds, then applying both sides to 1 gives $xa = ax$, *i.e.*, $a \in C(Q)$, and then $xy \cdot a = a \cdot xy = x \cdot ay = x \cdot ya$, *i.e.*, $a \in N_\rho(Q)$. □

The inner mapping group $\mathrm{Inn}(Q)$ of a loop Q has a standard set of generators

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

for $x, y \in Q$. The property of being an automorphic loop can therefore be expressed equationally by demanding that the permutations $L_{x,y}, R_{x,y}, T_x$ are homomorphisms. In particular, if Q is a commutative loop then Q is automorphic if and only if

$$(uv)L_{x,y} = uL_{x,y} \cdot vL_{x,y}$$

for every x, y, u, v.

In addition, we can conclude that (commutative) automorphic loops form a variety in the sense of universal algebra, and are therefore closed under subloops, products, and homomorphic images.

We will generally compute with translations whenever possible, but it will sometimes be convenient to work directly with the loop operations. Besides the loop multiplication, we also have the *left division* operation $\setminus : Q \times Q \to Q$ which satisfies

$$x \setminus (xy) = x(x \setminus y) = y\,.$$

The *division permutations* $D_x : Q \to Q$ defined by $yD_x = y \setminus x$ are also quite useful, as is the *inversion permutation* $J : Q \to Q$ defined by $xJ = xD_1 = x^{-1}$.

If Q is a commutative automorphic loop then for all $x, y \in Q$ we have

$$xL_{y,x} = x, \tag{2.1}$$
$$L_{y,x}L_{x^{-1}} = L_{x^{-1}}L_{y,x}, \tag{2.2}$$
$$yL_{y,x} = ((xy) \setminus x)^{-1}, \tag{2.3}$$
$$L_{x^{-1},y^{-1}} = L_{x,y}, \tag{2.4}$$
$$D_{x^2} = D_x J D_x, \tag{2.5}$$

where the first two equalities follow from [9, Lem. 2.3], (2.3) from [9, Lem 2.5], (2.4) is an immediate consequence of [9, Lem. 2.7], and (2.5) is [9, Lem. 2.8]. In addition, commutative automorphic loops satisfy the *automorphic inverse property*

$$(xy)^{-1} = x^{-1}y^{-1} \quad \text{and} \quad (x \setminus y)^{-1} = x^{-1} \setminus y^{-1}, \tag{2.6}$$

by [9, Lem. 2.6].

Finally, as in [9], in a commutative automorphic loop $(Q, \cdot)$, it will be convenient to introduce the permutations

$$P_x = L_x L_{x^{-1}}^{-1} = L_{x^{-1}}^{-1} L_x,$$

where the second equality follows from [9, Lem. 2.3].

Lemma 2.3. *For all x, y in a commutative automorphic loop $(Q, \cdot)$*

$$(x^{-1})P_{xy} = xy^2, \tag{2.7}$$
$$x \cdot xP_y = (xy)^2. \tag{2.8}$$

Proof. Equation (2.7) is from [9, Lem 3.2]. Replacing x with x^{-1} and y with xy in (2.7) yields $xP_{x^{-1}\cdot xy} = x^{-1}(xy)^2$ and $xP_{x^{-1}\cdot xy} = xL_{x,x^{-1}}P_{x^{-1}\cdot xy} = xL_{x,x^{-1}}P_{yL_{x,x^{-1}}}$. Now, for every automorphism φ of Q we have $x\varphi P_{y\varphi} = (y\varphi)^{-1} \setminus (y\varphi x\varphi) = (y^{-1} \setminus (yx))\varphi = xP_y\varphi$. Thus $x^{-1}(xy)^2 = xL_{x,x^{-1}}P_{yL_{x,x^{-1}}} = xP_yL_{x,x^{-1}}$. Canceling x^{-1} on both sides, we obtain (2.8). □

3 The associated Bruck loop

A loop $(Q, \circ)$ is said to be a (left) *Bol loop* if it satisfies the identity

$$(x \circ (y \circ x)) \circ z = x \circ (y \circ (x \circ z)) . \tag{3.1}$$

A Bol loop is a *Bruck loop* if it also satisfies the automorphic inverse property $(x \circ y)^{-1} = x^{-1} \circ y^{-1}$. (Bruck loops are also known as *K-loops* or *gyrocommutative gyrogroups*.)

The following construction is the reason for considering Bruck loops in this paper. Let $(Q, \cdot)$ be a uniquely 2-divisible commutative automorphic loop. Define a new operation $\circ$ on Q by

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

By [9, Lem. 3.5], $(Q, \circ)$ is a Bruck loop, and powers in $(Q, \circ)$ coincide with powers in $(Q, \cdot)$.

Since we will work with translations in both $(Q, \cdot)$ and $(Q, \circ)$, we will denote left translations in $(Q, \circ)$ by L_x°. For instance, we can express the fact that every Bol loop $(Q, \circ)$ is *left power alternative* by

$$(L_x^\circ)^n = L_{x^n}^\circ \tag{3.2}$$

for all integers n.

Proposition 3.1. *[12, Thm. 5.10] Let $(Q, \circ)$ be a Bol loop. Then $N_\lambda(Q, \circ) = N_\mu(Q, \circ)$. If, in addition, $(Q, \circ)$ is a Bruck loop, then $N_\lambda(Q, \circ) = Z(Q, \circ)$.*

In the uniquely 2-divisible case, we can say more about the center.

Lemma 3.2. *Let $(Q, \circ)$ be a uniquely 2-divisible Bol loop. Then $Z(Q, \circ) = C(Q, \circ) \cap N_\rho(Q, \circ)$.*

Proof. One inclusion is obvious. For the other, suppose $a \in C(Q, \circ) \cap N_\rho(Q, \circ)$. Then for all $x, y \in Q$,

$$\begin{aligned}(x^2 \circ a) \circ y &\overset{(3.2)}{=} (x \circ (x \circ a)) \circ y = (x \circ (a \circ x)) \circ y \\ &\overset{(3.1)}{=} x \circ (a \circ (x \circ y)) = x \circ (x \circ (a \circ y)) \\ &\overset{(3.2)}{=} x^2 \circ (a \circ y) ,\end{aligned}$$

where we used $a \in C(Q, \circ)$ in the second equality and Lemma 2.2 in the fourth. Since squaring is a permutation, we may replace x^2 with x to get $(x \circ a) \circ y = x \circ (a \circ y)$ for all $x, y \in Q$. Thus $a \in N_\mu(Q, \circ) = N_\lambda(Q, \circ)$ (Proposition 3.1), and so $a \in Z(Q, \circ)$. □

Lemma 3.3. *Let $(Q, \cdot)$ be a uniquely 2-divisible commutative automorphic loop with associated Bruck loop $(Q, \circ)$. Then $a \in Z(Q, \circ)$ if and only if, for all $x \in Q$,*

$$P_a P_x = P_x P_a . \tag{3.3}$$

Proof. By Lemmas 2.2 and 3.2, $a \in Z(Q, \circ)$ if and only if the identity $a \circ (x \circ y) = x \circ (a \circ y)$ holds for all $x, y \in Q$. This can be written as $[(y^2)P_x P_a]^{1/2} = [(y^2)P_a P_x]^{1/2}$. Squaring both sides and using unique 2-divisibility to replace y^2 with y, we have $(y)P_x P_a = (y)P_a P_x$ for all $x, y \in Q$. □

4 Proofs of the Main Results

Throughout this section, let $(Q, \cdot)$ be a uniquely 2-divisible, commutative automorphic loop with associated Bruck loop $(Q, \circ)$.

Lemma 4.1. *If $a \in Z(Q, \circ)$, then for all $x \in Q$,*

$$x L_{a \setminus x, a} = x L_{a \setminus x^{-1}, a} . \tag{4.1}$$

Proof. First,

$$\begin{aligned} x^{-2} = x^{-2}L_{a^{-1}}^{-1}L_{a^{-1}} &= a^{-1}D_{x^{-2}}L_{a^{-1}} \\ \overset{(2.6)}{=} aD_{x^2}JL_{a^{-1}} &\overset{(2.5)}{=} aD_xJD_xJL_{a^{-1}} \\ \overset{(2.6)}{=} aD_xD_{x^{-1}}L_{a^{-1}} &= (x^{-1})L_{a\setminus x}^{-1}L_{a^{-1}}\,. \end{aligned}$$

Thus we compute

$$\begin{aligned} (x^{-2})L_{a\setminus x,a} = (x^{-1})L_{a\setminus x}^{-1}L_{a^{-1}}L_{a\setminus x,a} &\overset{(2.2)}{=} (x^{-1})L_{a\setminus x}^{-1}L_{a\setminus x,a}L_{a^{-1}} \\ = (x^{-1})L_aL_x^{-1}L_{a^{-1}} &= aL_{x^{-1}}L_x^{-1}L_{a^{-1}} \\ = aP_{x^{-1}}L_{a^{-1}}\,, & \end{aligned} \tag{4.2}$$

Since $a^{-1} \in Z(Q,\circ)$, we may also apply (4.2) with a^{-1} in place of a, and will do so in the next calculation. Now

$$\begin{aligned} aP_{x^{-1}}L_{a^{-1}} = aP_{x^{-1}}P_{a^{-1}}L_a &\overset{(3.3)}{=} aP_{a^{-1}}P_{x^{-1}}L_a \\ = a^{-1}P_{x^{-1}}L_a &\overset{(4.2)}{=} (x^{-2})L_{a^{-1}\setminus x,a^{-1}} \\ \overset{(2.6)}{=} (x^{-2})L_{(a\setminus x^{-1})^{-1},a^{-1}} &\overset{(2.4)}{=} (x^{-2})L_{a\setminus x^{-1},a}\,, \end{aligned}$$

where we used $a^{-1} \in Z(Q,\circ)$ in the second equality.

Putting this together with (4.2), we have $(x^{-2})L_{a\setminus x,a} = (x^{-2})L_{a\setminus x^{-1},a}$ for all $x \in Q$. Since inner mappings are automorphisms, this implies $(xL_{a\setminus x,a})^{-2} = (xL_{a\setminus x^{-1},a})^{-2}$. Taking inverses and square roots, we have the desired result. □

Lemma 4.2. *If $a \in Z(Q,\circ)$, then for all $x \in Q$,*

$$(a\setminus x)L_{a\setminus x^{-1},a} = (x\setminus a)^{-1}, \tag{4.3}$$

$$x^{-1}\cdot xP_a = a^2. \tag{4.4}$$

Proof. We compute

$$(a\setminus x)L_{a\setminus x^{-1},a} = a\setminus(xL_{a\setminus x^{-1},a}) \overset{(4.1)}{=} a\setminus(xL_{a\setminus x,a}) \overset{(2.1)}{=} (a\setminus x)L_{a\setminus x,a} \overset{(2.3)}{=} (x\setminus a)^{-1}\,,$$

where we used $L_{a\setminus x^{-1},a} \in \mathrm{Aut}(Q)$ in the first equality and $L_{a\setminus x,a} \in \mathrm{Aut}(Q)$ in the third equality.

To show (4.4), we compute

$$\begin{aligned} x^{-1}\cdot xP_a = (x^{-1})L_{a^{-1}\setminus(ax)} &= (x^{-1})L_{a^{-1}\setminus(ax)}L_{a^{-1}}L_{ax}^{-1}L_{ax}L_{a^{-1}}^{-1} \\ = (a\setminus(ax))^{-1}L_{a^{-1}\setminus(ax),a^{-1}}L_{ax}L_{a^{-1}}^{-1} &\overset{(2.6)}{=} (a^{-1}\setminus(ax)^{-1})L_{a^{-1}\setminus(ax),a^{-1}}L_{ax}L_{a^{-1}}^{-1} \\ \overset{(4.3)}{=} ((ax)^{-1}\setminus a^{-1})^{-1}L_{ax}L_{a^{-1}}^{-1} &\overset{(2.6)}{=} ((ax)\setminus a)L_{ax}L_{a^{-1}}^{-1} \\ = aL_{a^{-1}}^{-1} &= a^2\,. \end{aligned}$$

Note that in the fifth equality, we are applying (4.3) with a^{-1} in place of a and $(ax)^{-1}$ in place of x. □

Lemma 4.3. *If $a \in Z(Q,\circ)$, then $L_a = L_a^\circ$, and for all integers n*

$$L_a^n = L_{a^n}. \tag{4.5}$$

Proof. For $x \in Q$, we compute

$$(a \circ x)^2 = (x \circ a)^2 = (a^2)P_x \overset{(4.4)}{=} xP_aL_{x^{-1}}P_x = x \cdot xP_a \overset{(2.8)}{=} (ax)^2 .$$

Taking square roots, we have $a \circ x = ax$, as desired. Then $L_a^n = (L_a^\circ)^n \overset{(3.2)}{=} L_{a^n}^\circ = L_{a^n}$. □

Lemma 4.4. *If $a \in Z(Q, \circ)$, then for all $x \in Q$,*

$$P_{xa} = P_xP_a . \tag{4.6}$$

Proof. For each $y \in Q$,

$$yP_{xa} = yP_{ax} = [ax \circ y^{1/2}]^2 = [(a \circ x) \circ y^{1/2}]^2 = [a \circ (x \circ y^{1/2})]^2 = yP_xP_a ,$$

using Lemma 4.3 in the third equality and $a \in Z(Q, \circ)$ in the fourth. □

Lemma 4.5. *If $a \in Z(Q, \circ)$, then $a^2 \in Z(Q, \cdot)$.*

Proof. We compute

$$\begin{aligned}
L_{a^2}L_x &\overset{(4.5)}{=} L_a^2L_x && = L_aL_{a,x}L_{xa} \\
&\overset{(2.4)}{=} L_aL_{a^{-1},x^{-1}}L_{xa} && = L_aL_{a^{-1}}L_{x^{-1}}L_{x^{-1}a^{-1}}^{-1}L_{xa} \\
&\overset{(4.5)}{=} L_{x^{-1}}L_{x^{-1}a^{-1}}^{-1}L_{xa} && \overset{(2.6)}{=} L_{x^{-1}}L_{(xa)^{-1}}^{-1}L_{xa} \\
&= L_{x^{-1}}P_{xa} && \overset{(4.6)}{=} L_{x^{-1}}P_xP_a \\
&= L_xL_aL_{a^{-1}}^{-1} && \overset{(4.5)}{=} L_xL_a^2 \\
&\overset{(4.5)}{=} L_xL_{a^2} .
\end{aligned}$$

By Lemma 2.2, it follows that $a^2 \in N_\rho(Q, \cdot)$, and $N_\rho(Q, \cdot) = Z(Q, \cdot)$ by Proposition 2.1. □

Lemma 4.6. *Let $(Q, \cdot)$ be a uniquely 2-divisible commutative automorphic loop with associated Bruck loop $(Q, \circ)$. Then $Z(Q, \circ) \subset Z(Q, \cdot)$.*

Proof. Assume that $a \in Z(Q, \circ)$. Then $a^2 \in Z(Q, \cdot)$ by Lemma 4.5, and thus $(aL_{x,y})^2 = a^2L_{x,y} = a^2$ for every $x, y \in Q$. Taking square roots yields $aL_{x,y} = a$, that is, $a \in Z(Q, \cdot)$. □

Now we prove Theorem 1.2, that is, we show that the upper central series of $(Q, \cdot)$ and $(Q, \circ)$ coincide.

Proof of Theorem 1.2. Since each $Z_n(Q)$ is the preimage of $Z(Q/Z_{n-1}(Q))$ under the canonical projection, it follows by induction that it suffices to show $Z(Q, \circ) = Z(Q, \cdot)$. One inclusion is Lemma 4.6. For the other, suppose $a \in Z(Q, \cdot)$. Then $P_aP_x = L_aL_{a^{-1}}^{-1}L_xL_{x^{-1}}^{-1} = L_xL_{x^{-1}}^{-1}L_aL_{a^{-1}}^{-1} = P_xP_a$, and so $a \in Z(Q, \circ)$ by Lemma 3.3. □

Proof of Theorem 1.1. For an odd prime p, let Q be a commutative automorphic p-loop with associated Bruck loop $(Q, \circ)$. By [6], $(Q, \circ)$ is centrally nilpotent of class, say, n. By Theorem 1.2, Q is also centrally nilpotent of class n. □

5 From anisotropic planes to automorphic p-loops with trivial nucleus

We proved in [10] that a commutative automorphic loop of order p, $2p$, $4p$, p^2, $2p^2$ or $4p^2$ is an abelian group. For every prime p there exist nonassociative commutative automorphic loops of order p^3. These loops have been classified up to isomorphism in [4], where the announced Theorem 1.1 has been used to guarantee nilpotency for p odd.

Without commutativity, we do not even know whether automorphic loops of order p^2 are associative! Nevertheless we show here that the situation is much more complicated than in the commutative case already for loops of order p^3. Namely, using anisotropic planes in the vector space $M(2,p)$ of 2×2 matrices over $GF(p)$, we construct a family of automorphic loops of order p^3 with trivial center.

5.1 Anisotropic planes

Let F be a field and $M(2,F)$ the vector space of 2×2 matrices over F. The determinant

$$\det : M(2,F)\to F,\quad \det\begin{pmatrix} a_1 & a_2\\ a_3 & a_4\end{pmatrix} = a_1a_4 - a_2a_3$$

is a quadratic form.

Recall that a subspace W of $M(2,F)$ is *anisotropic* if $\det(A)\neq 0$ for every $0\neq A\in W$. An anisotropic subspace of dimension two is called an *anisotropic plane*.

If $FC\oplus FD$ is an anisotropic plane in $M(2,F)$ then $C^{-1}(FC\oplus FD)$ is also anisotropic, and hence, while looking for anisotropic planes, it suffices to consider subspaces $FI\oplus FA$, where I is the identity matrix and $A\in GL(2,F)$.

Lemma 5.1. *With $A\in M(2,F)$, the subspace $FI\oplus FA$ is an anisotropic plane if and only if the characteristic polynomial $\det(A-\lambda I)=\lambda^2-\mathrm{tr}(A)\lambda+\det(A)$ has no roots in F.*

Proof. The subspace $FI\oplus FA$ is anisotropic if and only if $\det(\lambda I+\mu A)\neq 0$ for every λ, μ such that $(\lambda,\mu)\neq(0,0)$, or, equivalently, if and only if $\det(A-\lambda I)\neq 0$ for every λ. We have $\det(A-\lambda I)=\lambda^2-\mathrm{tr}(A)\lambda+\det(A)$. □

If F is algebraically closed, the characteristic polynomial of Lemma 5.1 will have roots and hence there are no anisotropic planes in $M(2,F)$. But it is easy to construct anisotropic planes in $M(2,\mathbb{R})$, for instance, by making sure that the discriminant $\mathrm{tr}(A)^2-4\det(A)$ is negative. We are now going to show that there are anisotropic planes (with additional properties) over every finite prime field.

A nonzero element $a\in GF(p)$ is a *quadratic residue* if $a=b^2$ for some $b\in GF(p)$. A nonzero element $a\in GF(p)$ that is not a quadratic residue is a *quadratic nonresidue*.

To guarantee existence of certain anisotropic planes we will need Lemma 5.3, which can easily be proved from the following strong results of Perron [16, Thms. 1 and 3] concerning additive properties of the set of quadratic residues:

Theorem 5.2. *[16] Let p be a prime, N_p the set of quadratic nonresidues, and $R_p=\{a\in GF(p);\ a \text{ is a quadratic residue or } a=0\}$.*

(i) If $p=4k-1$ and $a\neq 0$ then $|(R_p+a)\cap R_p|=k=|(R_p+a)\cap N_p|$.

(ii) If $p=4k+1$ and $a\neq 0$ then $|(R_p+a)\cap R_p|=k+1$, $|(R_p+a)\cap N_p|=k$.

Lemma 5.3. *For every prime $p\geq 7$ and every $a\neq 0$ there are $\lambda\neq 0$ and $\mu\neq 0$ such that λ^2+a is a quadratic residue and μ^2+a is quadratic nonresidue.*

Proof. We will use Theorem 5.2 without reference. Let $p=4k\pm 1$. If $k\geq 3$ then $|(R_p+a)\cap R_p|\geq 3$, so there is $\lambda\neq 0$ such that $0\neq\lambda^2+a\in R_p$. If $k\geq 2$ then $|(R_p+a)\cap N_p|\geq 2$, and since $0\notin N_p$, there is $\lambda\neq 0$ such that $\lambda^2+a\in N_p$. □

Lemma 5.4. *Let p be a prime and $F=GF(p)$.*

(i) There is $A \in GL(2,p)$ such that $\mathrm{tr}(A) = 0$ and $FI \oplus FA$ is anisotropic if and only if $p \neq 2$.

(ii) There is $A \in GL(2,p)$ such that $\mathrm{tr}(A) \neq 0$, $\det(A)$ is a quadratic residue modulo p and $FI \oplus FA$ is anisotropic if and only if $p \neq 3$.

(iii) There is $A \in GL(2,p)$ such that $\mathrm{tr}(A) \neq 0$, $\det(A)$ is a quadratic nonresidue modulo p and $FI \oplus FA$ is anisotropic if and only if $p \neq 2$.

Proof. (i): If $p \geq 3$, let a be a quadratic nonresidue and let

$$A = \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}.$$

Then $\mathrm{tr}(A) = 0$ and $\det(A - \lambda I) = \lambda^2 + \det(A) = \lambda^2 - a$ has no roots, so $FI \oplus FA$ is anisotropic by Lemma 5.1.

If $p = 2$, the only elements $A \in GL(2,p)$ with $\mathrm{tr}(A) = 0$ are

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Then $\det(A + I) = 0$, so $FI \oplus FA$ is not anisotropic by Lemma 5.1.

(ii) and (iii): Let $p \geq 3$ and let a and A be as above. For $\lambda \neq 0$ let

$$B_\lambda = A - \lambda I = \begin{pmatrix} -\lambda & 1 \\ a & -\lambda \end{pmatrix}.$$

Then $FI \oplus FB_\lambda = FI \oplus FA$ is anisotropic, $\mathrm{tr}(B_\lambda) = -2\lambda \neq 0$, and $\det(B_\lambda) = \lambda^2 - a$. If $p \geq 7$, Lemma 5.3 implies that there are $\lambda \neq 0$ and $\mu \neq 0$ such that $\det(B_\lambda)$ is a quadratic residue and $\det(B_\mu)$ is a quadratic nonresidue. If $p = 5$, the two matrices

$$C = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 1 \\ 3 & 1 \end{pmatrix}$$

are of the form B_λ with a suitable choice of a quadratic nonresidue a and a nonzero scalar λ. Moreover, $\mathrm{tr}(C) = \mathrm{tr}(D) \neq 0$, $\det(C) = 4$ is a quadratic residue and $\det(D) = 3$ is a quadratic nonresidue. If $p = 3$, the matrix C is again of the form B_λ for a suitable a and λ, $\mathrm{tr}(C) \neq 0$ and $\det(C) = 2$ is a quadratic nonresidue.

Let $p = 3$ and assume that E satisfies $\mathrm{tr}(E) \neq 0$, $\det(E)$ is a quadratic residue. Then $\det(E) = 1$, and $\det(E - \lambda I)$ is either $\lambda^2 + \lambda + 1$ (with root $\lambda = 1$) or $\lambda^2 - \lambda + 1$ (with root $\lambda = -1$), so $FI \oplus FE$ is not anisotropic by Lemma 5.1.

Finally assume that $p = 2$. Since every nonzero element of $GF(2)$ is a quadratic residue, we have (iii). On the other hand,

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

satisfies the conditions of (ii). □

5.2 Automorphic loops of order p^3 with trivial nucleus

Let $A \in GL(2,p)$ be such that $FI \oplus FA$ is an anisotropic plane. Define a binary operation on $F \times (F \times F)$ by

$$(a,x) \cdot (b,y) = (a + b, x(I + bA) + y(I - aA)) \tag{5.1}$$

and call the resulting groupoid $Q(A)$. Since

$$U_a = I + aA$$

is invertible for every $a \in F$, we see that $Q(A)$ is a loop (see Remark 5.8), and in fact, straightforward calculation shows that

$$(b,y)L_{(a,x)}^{-1} = (b-a,(y-xU_{b-a})U_{-a}^{-1}),$$
$$(b,y)R_{(a,x)}^{-1} = (b-a,(y-xU_{a-b})U_{a}^{-1}).$$

Lemma 5.5. *Let $F = GF(p)$. Let $A \in GL(2,p)$ be such that $FI \oplus FA$ is an anisotropic plane in $M(2,p)$. For each $z \in F \times F$ and each $C \in GL(2,p)$ satisfying $CA = AC$, define $\varphi_{z,C} : F \times (F \times F) \to F \times (F \times F)$ by*

$$(a,x)\varphi_{z,C} = (a, az + xC).$$

Then $\varphi_{z,C}$ is an automorphism of $Q(A)$.

Proof. We compute

$$\begin{aligned}(a,x)\varphi_{z,C} \cdot (b,y)\varphi_{z,C} &= (a,az+xC)\cdot(b,bz+yC)\\ &= (a+b,(az+xC)U_b + (bz+yC)U_{-a})\\ &= (a+b,(a+b)z + xCU_b + yCU_{-a} + abzA - abzA)\\ &= (a+b,(a+b)z + (xU_b + yU_{-a})C)\\ &= [(a,x)\cdot(b,y)]\varphi_{z,C},\end{aligned}$$

where we have used $CA = AC$ in the fourth equality. Since $\varphi_{z,C}$ is clearly a bijection, we have the desired result. □

Proposition 5.6. *Let $F = GF(p)$. Let $A \in GL(2,p)$ be such that $FI \oplus FA$ is an anisotropic plane in $M(2,p)$. Then the loop $Q = Q(A)$ is an automorphic loop of order p^3 and exponent p with $N_\mu(Q) = \{(0,x) \mid x \in F \times F\} \cong F \times F$ and $N_\lambda(Q) = N_\rho(Q) = 1$. In particular, $N(Q) = Z(Q) = 1$ and so Q is not centrally nilpotent. In addition, if $p = 2$ then $C(Q) = Q$, while if $p > 2$, then $C(Q) = 1$.*

Proof. Easy calculations show that the standard generators of the inner mapping group of $Q(A)$ are

$$\begin{aligned}(b,y)T_{(a,x)} &= (b,(x(U_{-b}-U_b)+yU_a)U_{-a}^{-1}),\\ (c,z)R_{(a,x),(b,y)} &= (c,(zU_aU_b + y(U_{-c-a}-U_cU_{-a}))U_{a+b}^{-1}),\\ (c,z)L_{(a,x),(b,y)} &= (c,(zU_{-a}U_{-b} + y(U_{c+a}-U_cU_a))U_{-a-b}^{-1}).\end{aligned} \tag{5.2}$$

Since $U_{-b} - U_b = -2bA$ and $U_{c+a} - U_cU_a = U_{-c-a} - U_cU_{-a} = -caA^2$, we find that each of these generators is of the form $\varphi_{u,C}$ for an appropriate $u \in F \times F$, $C \in GL(2,p)$ commuting with A. Specifically, we have

$$\begin{aligned}T_{(a,x)} &= \varphi_{u,C} \quad \text{where} \quad u = -2xAU_{-a}^{-1} \quad \text{and} \quad C = U_aU_{-a}^{-1},\\ R_{(a,x),(b,y)} &= \varphi_{u,C} \quad \text{where} \quad u = -ayA^2U_{a+b}^{-1} \quad \text{and} \quad C = U_aU_bU_{a+b}^{-1},\\ L_{(a,x),(b,y)} &= \varphi_{u,C} \quad \text{where} \quad u = -ayA^2U_{-a-b}^{-1} \quad \text{and} \quad C = U_{-a}U_{-b}U_{-a-b}^{-1}.\end{aligned}$$

By Lemma 5.5, it follows that $Q(A)$ is automorphic.

An easy induction shows that powers in $Q(A)$ and in $F \times (F \times F)$ coincide, so $Q(A)$ has exponent p.

Suppose that $(a,x) \in N_\mu(Q)$. Then $(c,z)R_{(a,x),(y,b)} = (c,z)$ for every $(c,z),(b,y)$. Thus $(zU_bU_a + y(U_{-c-a} - U_cU_{-a}))U_{a+b}^{-1} = z$ for every $(c,z),(b,y)$. With $z = 0$, we have $y(U_{-c-a} - U_cU_{-a}) = -cayA^2 = 0$ for every y, hence $caA^2 = 0$ for every c, and $a = 0$ follows. On the other hand, clearly $(0,x) \in N_\mu(Q)$ for every x. We have thus shown $N_\mu(Q) = \{(0,x) \mid x \in F \times F\} \cong F \times F$.

Suppose that $(c,z) \in N_\lambda(Q)$. Then $(c,z)R_{(a,x),(y,b)} = (c,z)$ for every $(a,x),(b,y)$. Thus $(zU_bU_a + y(U_{-c-a} - U_cU_{-a}))U_{a+b}^{-1} = z$ for every $(a,x),(b,y)$. With $y = 0$, we deduce that $zU_{a+b} = zU_aU_b$, or $abzA^2 = 0$ for every a,b. In particular, $zA^2 = 0$, and $z = 0$ follows. Then $y(U_{-c-a} - U_cU_{-a}) = -cayA^2 = 0$ for every

y, hence $caA^2 = 0$ for every a, and $c = 0$ follows. We have proved that $N_\lambda(Q) = 1$, and since $Q(A)$ is automorphic, $N_\rho(Q) = 1$ as well by Proposition 2.1.

If $p = 2$, then since $U_a = U_{-a}$, it follows that Q is commutative. Now assume that $p > 2$ and let $(a, x) \in C(Q)$. Then $x(U_b - U_{-b}) = y(U_a - U_{-a})$, that is, $2bxA = 2ayA$ for every $(b, y) \in Q$. With $b = 0$ we deduce that $2ayA = 0$ for every y, thus $0 = 2aA$, or $a = 0$. Then $2bxA = 0$, and with $b = 1$ we deduce $2xA = 0$, or $x = 0$. We have proved that $C(Q) = 1$. □

Remark 5.7. *The construction $Q(A)$ works for every real anisotropic plane $\mathbb{R}I \oplus \mathbb{R}A$ and results in an automorphic loop on $\mathbb{R}^3$ with trivial center. We believe that this is the first time a smooth nonassociative automorphic loop has been constructed.*

Remark 5.8. *The groupoid $Q(A)$ is an automorphic loop as long as $I + aA$ is invertible for every $a \in F$, which is a weaker condition than having $FI \oplus FA$ an anisotropic plane, as witnessed by $A = 0$, for instance.*

Let us assume that $A \in M(2, F)$ is such that $I + aA$ is invertible for every $a \neq 0$ but $FI \oplus FA$ is not anisotropic. Then $\det(A) = 0$ and $\det(A - \lambda I) = \lambda^2 - \mathrm{tr}(A)\lambda = \lambda(\lambda - \mathrm{tr}(A))$ has no nonzero solutions. Hence $\mathrm{tr}(A) = 0$, and there are $u \in F$ and $0 \neq v \in F$ such that

$$A = \begin{pmatrix} u & v \\ -\frac{u^2}{v} & -u \end{pmatrix} \quad or \quad A = \begin{pmatrix} u & -\frac{u^2}{v} \\ v & -u \end{pmatrix}. \tag{5.3}$$

In particular, $A^2 = 0$. The loop $Q = Q(A)$ is still an automorphic loop by the argument given in the proof of Proposition 5.6, and we claim that it is a group. Indeed, we have $(c, z) \in N_\lambda(Q) = N(Q)$ if and only if $(c, z) = (c, z)R_{(a,x),(b,y)}$ for every (a, x), (b, y), that is, by (5.2),

$$z = (zU_aU_b + y(U_{-c-a} - U_{-c}U_{-a}))U_{a+b}^{-1} \tag{5.4}$$

for every (a, x), (b, y). As $U_{b+a} - U_bU_a = -baA^2 = 0$ for every a, b, we see that equation (5.4) holds, $(c, z) \in N(Q)$, and Q is a group.

6 Open problems

Problem 6.1. *Are the following two statements equivalent for a finite automorphic loop Q?*

(i) Q has order a power of 2.

(ii) Every element of Q has order a power of 2.

Problem 6.2. *Let p be a prime. Are all automorphic loops of order p^2 associative?*

Problem 6.3. *Let p be a prime. Is there an automorphic loop of order a power of p and with trivial middle nucleus?*

Problem 6.4. *Let p be a prime. Are there automorphic loops of order p^3 that are not centrally nilpotent and that are not constructed by Proposition 5.6?*

Conjecture 6.5. *Let p be a prime and $F = GF(p)$. Call an element $A \in GL(2, p)$ of* type 1 *if $\mathrm{tr}(A) = 0$, of* type 2 *if $\mathrm{tr}(A) \neq 0$ and $\det(A)$ is a quadratic residue, and of* type 3 *if $\mathrm{tr}(A) \neq 0$ and $\det(A)$ is a quadratic nonresidue.*

Let $A, B \in GL(2, p)$ be such that $FI \oplus FA$ and $FI \oplus FB$ are anisotropic planes. Then the loops $Q(A)$, $Q(B)$ constructed by (5.1) are isomorphic if and only if they are of the same type.

We have verified Conjecture 6.5 computationally for $p \leq 5$. Taking advantage of Lemma 5.4, we can therefore conclude:

If $p = 2$, there is one isomorphism type of loops $Q(A)$ obtained from the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

of type 2. This is the unique commutative automorphic loop of order 8 that is not centrally nilpotent, constructed already in [10]. If $p = 3$, there are two isomorphism types of loops $Q(A)$, corresponding to

$$\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

of types 1 and 3, respectively. If $p = 5$, there are three isomorphism types. If Conjecture 6.5 is valid for a prime $p > 5$, then there are three isomorphism types of loops $Q(A)$ for that prime p, according to Lemma 5.4.

Acknowledgment We are pleased to acknowledge the assistance of Prover9 [15], an automated deduction tool, Mace4 [15], a finite model builder, and the GAP [5] package Loops [17]. Prover9 was indispensable in the proofs of the lemmas leading up to Theorem 1.2. We used Mace4 to find the first automorphic loop of exponent 3 with trivial center in §5. We used the Loops package to verify Conjecture 6.5 for $p \leq 5$.

References

[1] V. D. Belousov, *Foundations of the Theory of Quasigroups and Loops*, Izdat. Nauka, Moscow, 1967 (Russian).

[2] R. H. Bruck, *A Survey of Binary Systems*, Springer-Verlag, 1971.

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

[4] D. A. S. de Barros, A. Grishkov and P. Vojtěchovský, Commutative automorphic loops of order p^3, *J. Algebra Appl.* **11**,5 (2012), 15 pages

[5] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.10*; 2007, (`http://www.gap-system.org`)

[6] G. Glauberman, On loops of odd order I, *J. Algebra* **1** (1964), 374–396.

[7] G. Glauberman, On loops of odd order II, *J. Algebra* **8** (1968), 393–414.

[8] G. Glauberman and C. R. B. Wright, Nilpotence of finite Moufang 2-loops. *J. Algebra* **8** (1968), 415–417.

[9] P. Jedlička, M. K. Kinyon and P. Vojtěchovský, The structure of commutative automorphic loops, *Trans. Amer. Math. Soc.* **363** (2011), 365–384.

[10] P. Jedlička, M. K. Kinyon and P. Vojtěchovský, Constructions of commutative automorphic loops, *Comm. Algebra* **38**, 9 (2010), 3243–3267

[11] K. W. Johnson, M. K. Kinyon, G. P. Nagy and P. Vojtěchovský, Searching for small simple automorphic loops, *LMS J. Comput. Math.* **14** (2011), 200–213

[12] H. Kiechle, *The Theory of K-loops*, Lecture Notes in Math. **1778**, Springer-Verlag, Berlin, 2002.

[13] K. Kunen, M. K. Kinyon, J. D. Phillips and P. Vojtěchovský, The structure of automorphic loops, *Trans. Amer. Math. Soc.*, to appear

[14] M. Kinyon, J. D. Phillips and Vojtěchovský, When is the commutant of a Bol loop a subloop? *Trans. Amer. Math. Soc.* **360** (2008), no. 5, 2393–2408.

[15] W. McCune, *Prover9 and Mace4*, version 2009-11A, (`http://www.cs.unm.edu/ mccune/prover9/`)

[16] O. Perron, *Bemerkungen über die Verteilung der quadratischen Reste*, Mathematische Zeitschrift **56** (1952), no. **2**, 122–130.

[17] G. Nagy and P. Vojtěchovský, *LOOPS: Computing with quasigroups and loops in GAP* – a GAP package, version 2.0.0, 2008, (`http://www.math.du.edu/loops`)

[18] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math. **8**, Heldermann Verlag, Berlin, 1990.

5 On commutative A-loops of order pq

Přemysl Jedlička, Denis Simon

Abstract

We study a construction introduced by Aleš Drápal, giving raise to commutative A-loops of order kn where k and n are odd numbers. We show which combinations of k and n are possible if the construction is based on a field or on a cyclic group. We conclude that if p and q are odd primes, there exists a non-associative commutative A-loop of order pq if and only if p divides $q^2 - 1$ and such a loop is most probably unique.

1 Introduction

A *loop* is a quasigroup with a neutral element 1. An *inner mapping* of a loop is any composition of left and right translations (i.e. mappings $x \mapsto ax$ and $x \mapsto xa$) that fixes 1. If all inner mappings of a loop are automorphisms then the loop is called an *A-loop*. In spite of the fact that A-loops were introduced in the 50's [2], a more thorough investigation started only in recent years, see e.g. [8], [6], [7].

There are still not many examples of proper A-loops. For instance the only known commutative A-loops that are neither p-loops nor direct products were introduced by Aleš Drápal in [5] but the article did not specify what orders can and what orders cannot be achieved via this construction.

We partially fill the gap. Whereas Drápal's construction is based upon an arbitrary commutative ring, we focus our attention on the rings $\mathbb{Z}/n\mathbb{Z}$ only. This is done in two steps. First we consider the p-element fields; it turns out that all the construction works exactly the same way for any fields and hence the proofs are pronounced in a general setting. In the second step we study general rings $\mathbb{Z}/n\mathbb{Z}$. In fact, we always consider n to be odd due to the following result: Kinyon, Vojtěchovský and the first author proved in [6] that every finite commutative A-loop is the direct product of its 2-component and a loop of odd order. Commutative A-loops which are 2-loops were intensively studied in [7]. Hence in this paper, we do not consider any ring where 2 is not invertible.

Our main result is the description of all non-associative A-loop orders that can be obtained if Drápal's construction is based upon a field or upon $\mathbb{Z}/n\mathbb{Z}$. For instance, a non-associative loop based upon a field of size q can only have $k \cdot q$ elements, where k is an odd divisor either of $q - 1$ or of $q + 1$. Moreover, such a loop is unique (based on this construction). As a corollary we conclude that there exists a non-associative commutative A-loop of order pq, $p < q$ odd primes, if and only if p divides $q^2 - 1$ and we give an argument why we think that such a loop is the only commutative A-loop of order pq, up to isomorphism.

An interesting feature of the paper is that although it establishes some facts in loop theory, except for the last section we do not consider loops *en soi*. We work (nearly) entirely within the scope of fields or number rings. Hence the paper could well be read by someone not interested in loop theory.

The paper is organised as follows. In Section we introduce the construction, especially so-called 0-bijective fractional linear mappings which are the ground stone of the construction. In Section we study these mappings in the context of projective spaces over fields which gives us necessary and sufficient conditions for the mappings to exist. In Section we do the same work not upon fields but upon rings $\mathbb{Z}/n\mathbb{Z}$ which, of course, heavily depends on the results of Section . In Section we prove that, in fields, A-loops of the same order obtained via different invertible coefficients have to be isomorphic and hence there exists a unique loop for each order. Finally, in Section we deal with the case of commutative A-loops of order pq and their associated Bruck loops.

2 Drápal's construction

In this section we present a construction of loops introduced by Drápal in [5]. These loops were constructed so that their inner mapping groups are metacyclic. We give some properties of the construction here and we clarify the aims of this paper. For the definition of a loop, a standard reference is [1]. Nevertheless, it should suffice to know that loops are "groups without associativity". We start with the definition of a mapping which is bijective on the orbit containing 0.

Definition 2.1. 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

1. $f^i(0)$ is defined for each $i \geq 1$;
2. for each $i \geq 1$ there exists a unique $y \in R$ such that $f^i(y)$ is defined and equal to 0—we denote this element $f^{-i}(0)$; and
3. $f(0) \in R^*$.

We say that a 0-bijective partial mapping f is of 0-*order* k, if k is the smallest positive integer such that $f^k(0) = 0$. We say that it is of 0-order ∞ if $f^k(0) \neq 0$ for all k.

In fact these 0-bijections are the structure we study through the entire article, but only those which can be given by a formula $f(x) = (sx + 1)/(tx + 1)$, for some elements s and t in R, with $s - t$ invertible. We shall denote these mappings $f_{s,t}$. They serve for the following construction:

Proposition 2.1 (Drápal [5])**.** *Let M be a module over a commutative ring R and let $f_{s,t} : R \to R$, for some $s, t \in R$ with $s - t \in R^*$, be a 0-bijective mapping of 0-order k. Then we can define a commutative loop Q on the set $M \times \mathbb{Z}/k\mathbb{Z}$ as follows:*

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

The loop is denoted $M[s, t]$. Its inner mapping group is the semidirect product $tM \rtimes G$, where $G = \left\langle 1 + t f^i(0) f^j(0) \right\rangle \leq R^*$.

Example 2.2. *Let M be a module over a commutative ring R where 2 is invertible. Let $s = 1$ and $t = -3$. Then it is easy to see that $f^3_{1,-3}(0) = 0$ and hence $M[1, -3]$ is a loop defined on the set $M \times \mathbb{Z}/3\mathbb{Z}$.*

We have not said yet that the construction gives something non-trivial, i.e. that we obtain non-associative loops. It is almost always the case:

Proposition 2.3 (Drápal [5])**.** *Let $Q = M[s, t]$ where M is a faithful module over a commutative ring R. If $t \neq 0$ then Q is not associative, otherwise Q is a group.*

As we already said in the introduction, our main aim is to describe A-loops that can be obtained via this construction. From this point of view, the most interesting is the case $s = 1$.

Theorem 2.4 (Drápal [5])**.** *Let $Q = M[s, t]$ where M is faithful module over a commutative ring R. If $s = 1$ then Q is an A-loop. On the other hand, if $t \in R^*$ and Q is an A-loop then $s = 1$.*

Hence theoretically the construction gives many possible A-loops. The natural questions that arise are as follows.

Question 1: Given a commutative ring R, which numbers k can appear as a 0-order of some 0-bijective mapping $f_{1,t}$?

Question 2: Given a commutative ring R and a number k, for which t does there exist a 0-bijective mapping $f_{1,t}$ of the prescribed 0-order k?

These questions were left unanswered in [5], and so we address them here.

3 Orders of the mappings in fields

This section is the core of the paper. We are interested in describing the 0-orders of mappings $f_{s,t}$ when the base ring is $\mathbb{Z}/n\mathbb{Z}$. Naturally, the first case to consider is when $n = p$ is a prime number, that is $\mathbb{Z}/p\mathbb{Z}$ is the p-element field $\mathbb{F}_p$. It turns out that there is not much difference between the behaviour of $f_{s,t}$ on p-element fields and general fields. Hence we can consider K to be any field and we can even present infinite examples. The only difference for infinite fields is the possibility to have infinite 0-orders. Such orders will be usually ignored since they cannot appear in finite fields.

We investigate here the questions stated in the previous section giving answers to each of them, in the case of fields only, of course. We start the section in a more general setting considering s to be arbitrary because the proofs given do not much depend on s. However, at the end of the section, there is a result that we can prove only for $s = 1$.

In the entire section we shall work in a field K with characteristic different from 2. It was observed already in [5] that a mapping $f_{s,t} = \frac{sx+1}{tx+1}$, with $s \neq t$ can be viewed as an automorphism of the projective line $\mathbb{P}^1(K)$ over K given by the matrix

$$F_{s,t} = \begin{pmatrix} s & 1 \\ t & 1 \end{pmatrix}$$

(we drop the indices when they are evident from the context). Hence we can translate the notion of 0-order to automorphisms of projective lines. But we shall be a bit more careful since an automorphism is always a 0-bijection.

Definition 3.1. Let F be an automorphism of the projective line $\mathbb{P}^1(K)$. We say that F is of *projective 0-order* k if k is the smallest positive integer such that $F^k\binom{0}{1} = \binom{0}{x}$, for some $x \in K^*$.
We say that F *meets infinity* at ℓ, if $F^\ell\binom{0}{1} = \binom{x}{0}$, for some $x \in K^*$. We say simply that F meets infinity if there is some ℓ at which it happens.
We say that F is of *0-order* k if F is of projective 0-order k and never meets infinity.

It is immediate from the definition that a mapping $f_{s,t}$ is of 0-order k if and only if the corresponding automorphism $F_{s,t}$ is of 0-order k. First of all, we shall get rid of trivial cases:

Lemma 3.1. *The projective 0-order of $F_{s,t}$ can never be equal to 1.*

Proof. This is because $F\binom{0}{1} = \binom{1}{1}$. □

Lemma 3.2. *Let s and t be distinct elements of K. The projective 0-order of $F_{s,t}$ is $k = 2$ if and only if $s = -1$. If $s = -1$, then $F_{-1,t}$ does not meet infinity.*

Proof. From the relation $F^2 = \begin{pmatrix} s^2+t & s+1 \\ st+t & t+1 \end{pmatrix}$ it is clear that the projective 0-order of F is 2 if and only if $s = -1$. Since $F\binom{0}{1} = \binom{1}{1}$, we see that F does not meet infinity at 1, hence, by periodicity, $F_{-1,t}$ never meets infinity. □

From now on, we will assume that $s \neq -1$, and hence that the projective 0–order of $F_{s,t}$ is $k > 2$.

Let $\lambda = \lambda_{s,t}$ and $\mu = \mu_{s,t}$ be the eigenvalues of the matrix $F_{s,t}$ These are the roots of the characteristic polynomial $P_{s,t} = x^2 - (s+1)x + s - t$ and belong to the algebraic closure of K (in fact they belong to an at most quadratic extension of K). They satisfy $\lambda + \mu = s + 1$ and $\lambda\mu = s - t$. Since $s \neq t$, none of the eigenvalues can be 0. The discriminant of P is

$$D_{s,t} = (s-1)^2 + 4t \ .$$

This value is $D_{s,t} = 0$ if and only if $t = -\left(\frac{s-1}{2}\right)^2$. This is the case we investigate first.

Proposition 3.3. *Assume that $t = -\left(\frac{s-1}{2}\right)^2$ and $s \neq -1$.*
The projective 0-order of $F_{s,t}$ depends on the characteristic of the field K and is equal to

$$k = \begin{cases} p & \text{if } \operatorname{char}(K) = p, (p \neq 2) \\ \infty & \text{if } \operatorname{char}(K) = 0 \end{cases}$$

If $s = 1$, then $F_{1,0}$ does not meet infinity.

If $s \neq 1$, then $F_{s,t}$ meets infinity at ℓ if and only if $\ell = 1 + \frac{2}{s-1}$. In particular, in odd characteristic p it meets infinity if and only if s belongs to the prime field $\mathbb{F}_p$.

Proof. We first remark that the assumption $s \neq -1$ implies that $t \neq s$. We have $F = \frac{s+1}{2} \cdot I + N$, where $N = \begin{pmatrix} (s-1)/2 & 1 \\ -(s-1)^2/4 & -(s-1)/2 \end{pmatrix}$ and I is the identity matrix. Note that $N^2 = 0$ and that $\frac{s+1}{2}$ is invertible in K. Hence, using binomial expansion, we get $F^i = \left(\frac{s+1}{2}\right)^i \cdot I + i \cdot \left(\frac{s+1}{2}\right)^{i-1} \cdot N$. The first coordinate of the vector $F^i\binom{0}{1}$ is then $i \cdot \left(\frac{s+1}{2}\right)^{i-1}$ which is zero if and only if i is zero, whence the value of the projective 0-order.

The second coordinate of $F^i\binom{0}{1}$ is $\left(\frac{s+1}{2}\right)^i + i \cdot \left(\frac{s+1}{2}\right)^{i-1} \cdot \left(-\frac{s-1}{2}\right)$ which is equal to zero if and only if $i = 1 + \frac{2}{s-1}$ (if $s = 1$, this is never equal to zero).

In odd characteristic p, the conclusion is clear from the relation $i = 1 + \frac{2}{s-1}$. □

The previous proposition is in fact interesting in the case $s \neq 1$ only. Indeed, if $s = 1$ and $t = -(\frac{s-1}{2})^2$ then $t = 0$. But the choice $t = 0$ gives raise to a group, according to Proposition 2.3.

We are now finished with the case $D_{s,t} = 0$ and we can proceed with the generic case $D_{s,t} \neq 0$, i.e. $\lambda \neq \mu$. We recall that from the relation $\lambda\mu = s - t$, we have seen that λ and μ cannot be equal to 0.

Proposition 3.4. *Assume that $D_{s,t} \neq 0$. For $i \geq 0$ we have*

$$F^i_{s,t}\binom{0}{1} = \begin{pmatrix} \frac{\lambda^i - \mu^i}{\lambda - \mu} \\ \frac{\lambda^i(1-\mu) - \mu^i(1-\lambda)}{\lambda - \mu} \end{pmatrix}.$$

The projective 0-order of $F_{s,t}$ is equal to the order of $\frac{\lambda}{\mu}$ in the multiplicative group $\overline{K}^*$, that is the smallest positive integer such that $\left(\frac{\lambda}{\mu}\right)^k = 1$.

If $t = 0$, then $F_{s,0}$ does not meet infinity. If $t \neq 0$, then $\lambda - 1$ and $\mu - 1$ are both nonzero, and the mapping $F_{s,t}$ meets infinity at ℓ if $\left(\frac{\lambda}{\mu}\right)^\ell = \frac{\lambda-1}{\mu-1}$.

Proof. Since F has two distinct eigenvalues, there exists a regular matrix S, with coefficients in $\overline{K}$, such that $F = S\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}S^{-1}$. Hence $F^i\binom{0}{1} = S\begin{pmatrix} \lambda^i & 0 \\ 0 & \mu^i \end{pmatrix}S^{-1}\binom{0}{1} = \lambda^i A + \mu^i B$ for some vectors A and B. From the independent linear relations $F^0\binom{0}{1} = A + B = \binom{0}{1}$ and $F^1\binom{0}{1} = \lambda A + \mu B = \binom{1}{1}$, we find the solution

$$A = \begin{pmatrix} \frac{1}{\lambda-\mu} \\ \frac{1-\mu}{\lambda-\mu} \end{pmatrix}, \qquad B = \begin{pmatrix} \frac{-1}{\lambda-\mu} \\ -\frac{1-\lambda}{\lambda-\mu} \end{pmatrix},$$

giving the first part of the proposition.

The projective 0-order of F is the smallest positive integer k such that $F^k\binom{0}{1} = \binom{0}{x}$. From the previous relation, this is the smallest positive integer such that $\frac{\lambda^k - \mu^k}{\lambda - \mu} = 0$ and hence $\lambda^k = \mu^k$.

By definition, F meets infinity at ℓ if $F^\ell\binom{0}{1} = \binom{x}{0}$. From the previous relation, this is equivalent to $\frac{\lambda^\ell(1-\mu) - \mu^\ell(1-\lambda)}{\lambda - \mu} = 0$. We have $(1 - \lambda)(1 - \mu) = P(1) = -t$. If $t = 0$ then $P(1) = 0$ hence either $\lambda = 1$ or $\mu = 1$ (but not both). By symmetry, we may assume that $\mu = 1$ and $\lambda \neq 1$. In this case, the condition that F meets infinity at ℓ simplifies to $1 = 0$, which is clearly impossible. When $t \neq 0$, we have $P(1) \neq 0$, hence λ and μ are different from 1. In this case, the condition that F meets infinity at ℓ simplifies to $\left(\frac{\lambda}{\mu}\right)^\ell = \frac{1-\lambda}{1-\mu}$. □

This proposition gives us a first answer to Question 1 stated in Section 2 when the base ring is a field.

Corollary 3.5. *Let $F_{s,t}$ be a mapping defined over a field K (of odd characteristic), such that $D_{s,t} \neq 0$. Assume that $F_{s,t}$ has projective 0-order $k > 2$.*

- *If $D_{s,t}$ is a square in K, then K contains a primitive k-th root of unity.*
- *If $D_{s,t}$ is not a square in K, then the quadratic extension $K(\sqrt{D_{s,t}})$ contains a primitive k-th root of unity of norm 1.*

Proof. From Proposition 3.4, it is immediate that $\frac{\lambda}{\mu}$ is a primitive k-th root of unity in $K(\sqrt{D})$. If D is not a square in K, then the eigenvalues λ and μ are conjugate in the quadratic extension $K(\sqrt{D})$, hence $\frac{\lambda}{\mu}$ has norm 1. □

In order to apply this corollary to a finite field, it is useful to have the following description of the roots of unity in finite fields:

Proposition 3.6. *Let $K = \mathbb{F}_q$ with $q = p^n$ ($p \neq 2$). For an integer $k > 0$, we have*

- *$\mathbb{F}_q$ contains a primitive k-th root of unity if and only if k is a divisor of $q - 1$.*
- *$\mathbb{F}_{q^2}$ contains a primitive k-th root of unity of norm 1 in the extension $\mathbb{F}_{q^2}/\mathbb{F}_q$ if and only if k is a divisor of $q + 1$.*

Proof. The first assertion is an immediate consequence of the fact that the multiplicative group $\mathbb{F}_q^*$ is cyclic of order $q-1$. Consider now the second assertion. The norm map is a surjective homomorphism $\mathbb{F}_{q^2}^* \twoheadrightarrow \mathbb{F}_q^*$, hence its kernel is a subgroup of $\mathbb{F}_{q^2}^*$, of order $(q^2-1)/(q-1) = q+1$. This kernel is therefore the cyclic subgroup of order $q+1$, whence the conclusion. □

By Corollary 3.5, we have given a partial answer to Question 1. In order to prove that this is actually a complete answer, we need to study the converse property, and to answer Question 2.

Proposition 3.7. *Assume that the field K contains a primitive k–th root of unity for $k > 2$. Then, for each $s \in K$, $s \neq -1$, there exist exactly $\varphi(k)/2$ choices of $t \in K$ such that $F_{s,t}$ is of projective 0-order k, namely $t = \frac{(\zeta-s)(s\zeta-1)}{(\zeta+1)^2}$, where ζ is any primitive k-th root of unity.*

Remark 3.8. *In this proposition, $\varphi(k)$ denotes Euler's function.*

Proof. Assume that $F_{s,t}$ is of projective 0-order $k > 2$. Then by Proposition 3.4, the quotient of the eigenvalues $\zeta = \frac{\lambda}{\mu}$ is a primitive k–th root of unity. We have the relations $\lambda = \zeta\mu$ and $\lambda + \mu = s + 1$, hence $\mu = \frac{s+1}{\zeta+1}$ and $\lambda = \frac{\zeta(s+1)}{\zeta+1}$. From this we get $s - t = \lambda\mu = \zeta\frac{(s+1)^2}{(\zeta+1)^2}$, whence $t = \frac{(\zeta-s)(s\zeta-1)}{(\zeta+1)^2}$.

Conversely, assume that $t = \frac{(\zeta-s)(s\zeta-1)}{(\zeta+1)^2}$, where ζ is a primitive k-th root of unity in K. With this choice, we have $(x - \frac{s+1}{\zeta+1})(x - \frac{\zeta(s+1)}{\zeta+1}) = x^2 - (s+1)x + s - \frac{(\zeta-s)(s\zeta-1)}{(\zeta+1)^2} = P_{s,t}$. According to Proposition 3.4, the projective 0-order of $F_{s,t}$ is the smallest k' such that $\left(\frac{s+1}{\zeta+1}\right)^{k'} = \left(\frac{\zeta(s+1)}{\zeta+1}\right)^{k'}$ or equivalently such that $1 = \zeta^{k'}$. By definition of ζ, the projective 0–order of $F_{s,t}$ is exactly k.

In order to finish the proof, it only remains to prove that the map $\zeta \mapsto t$ is 2-to-1, since there are exactly $\varphi(k)$ primitive k-th roots of unity in K.

We have $t = \frac{(\zeta-s)(s\zeta-1)}{(\zeta+1)^2} = \left(\frac{(s+1)(\zeta-1)}{2(\zeta+1)}\right)^2 - \left(\frac{s-1}{2}\right)^2$. We look at the equality the other way round saying

$$\frac{\zeta-1}{\zeta+1} = \pm\frac{2}{s+1}\cdot\sqrt{t + \left(\frac{s-1}{2}\right)^2} = \pm\frac{2}{\lambda+\mu}\cdot\sqrt{\frac{D}{4}} = \pm\frac{2}{\lambda+\mu}\cdot\frac{\lambda-\mu}{2} = \pm\frac{\lambda-\mu}{\lambda+\mu}$$

which leads to $\zeta = \lambda/\mu$ or $\zeta = \mu/\lambda$. This proves that two different values of ζ give rise to the same value of t if and only if they are inverse to one other, and that the map $\zeta \mapsto t$ is 2-to-1 when $k > 2$. □

Example 3.9. *Let $K = \mathbb{C}$. Then, for any s and k, there exists $F_{s,t}$ of projective 0-order k since all k-th roots of 1 lie in $\mathbb{C}$. Furthermore, if we consider $s = 1$ and $t = 4$, the corresponding eigenvalues are $\lambda = -1$ and $\mu = 3$, hence $\frac{\lambda}{\mu}$ is not a root of unity in $\mathbb{C}$ and $F_{1,4}$ has projective 0-order $k = \infty$. A counting argument proves that almost every choice of s and t gives an $F_{s,t}$ with infinite projective 0-order.*

Proposition 3.10. *Assume that a quadratic extension L of K contains a primitive k–th root of unity for $k > 2$, of norm 1. Then, for each $s \in K$, $s \neq -1$, there exist exactly $\varphi(k)/2$ choices of $t \in K$ such that $F_{s,t}$ is of projective 0-order k, namely $t = \frac{(\zeta-s)(s\zeta-1)}{(\zeta+1)^2}$, where ζ is any primitive k-th root of unity in L.*

Proof. Everything in this proposition is already contained in Proposition 3.7 (applied to the field L), except that the given formula for t indeed gives an element of K when $s \in K$ and ζ has norm 1. Let $\overline{\zeta}$ and $\overline{t}$ be the conjugates of ζ and t in the extension L/K. We have $\zeta\overline{\zeta} = 1$. Starting from the definition of $\overline{t}$ and multiplying the numerator and the denominator by ζ^2, we obtain

$$\overline{t} = \frac{(\overline{\zeta} - s)(s\overline{\zeta} - 1)}{(\overline{\zeta} + 1)^2} = \frac{(1 - s\zeta)(s - \zeta)}{(1 + \zeta)^2} = t \, .$$

□

Remark 3.11. *This result suggests a more symmetrical expression for t:*

$$t = -\frac{(\zeta - s)(\zeta^{-1} - s)}{(\zeta + 1)(\zeta^{-1} + 1)} \, .$$

Putting things together, we have now a complete answer to Questions 1 and 2 in the case of fields. In fact, this result is only concerned with the projective 0-order and not the general 0-order, that is it does not say anything about the question of meeting infinity. We shall answer this question later but only when $s = 1$.

Theorem 3.12. *Let K be a field and $s \neq -1$ be any element of K. Let $k > 2$ be an integer and assume that $\mathrm{char}(K) \nmid 2k$. There exists $t \in K$ such that $F_{s,t}$ is of projective 0-order k if and only if a primitive k-th root of unity*

- *either lies in K*
- *or lies in a quadratic extension of K and is of norm 1 with respect to K.*

If one of these conditions is fulfilled then there exist exactly $\varphi(k)/2$ choices of t, namely $t = \frac{(\zeta-s)(s\zeta-1)}{(\zeta+1)^2}$, where ζ is a primitive k-th root of unity.

Example 3.13. *Let us take $K = \mathbb{R}$. For every $k > 2$, the k-th roots of unity are complex numbers of norm 1 and hence, for every $s \neq -1$, there exists a $t \in \mathbb{R}$ such that $F_{s,t}$ is of projective 0-order k. This value of k is obtained for example for $s = 1$ and $t = -\frac{1-\cos(2\pi/k)}{1+\cos(2\pi/k)} = -\tan^2(\pi/k)$.*

Example 3.14. *Let us take $K = \mathbb{Q}$. A primitive k-th root of unity lies in a quadratic extension of $\mathbb{Q}$ if and only if $k = 3$, 4, or 6. Hence the only possible finite projective 0-orders are respectively 3, 4, and 6. These values are made possible for example by the values $s = 1$ and respectively $t = -3$, $t = -1$, and $t = -1/3$.*

Now we are done with examining the projective 0-order and it is time to study when $F_{s,t}$ meets infinity. However it does not seem to be easy to solve, except in the case $s = 1$. The mapping $F_{1,0}$ was studied in Proposition 3.3.

Lemma 3.15. *Let $t \neq 0$ be an element of K. Assume that $F_{1,t}$ is of projective 0-order k. Then $F_{1,t}$ meets infinity at ℓ if and only if k is a finite even integer and ℓ is an odd multiple of $k/2$.*

Proof. According to Proposition 3.4, $F_{1,t}$ meets infinity at ℓ if $(\lambda/\mu)^\ell = (\lambda - 1)/(\mu - 1)$. Under the condition $s = 1$, λ and μ are roots of the polynomial $P_{1,t}$ that can be rewritten as $P_{1,t} = (x-1)^2 - t$, which implies that $\lambda - 1$ and $\mu - 1$ are equal to $\pm\sqrt{t}$. In particular, the quotient $(\lambda - 1)/(\mu - 1)$ is equal to -1. We deduce from the relation $(\lambda/\mu)^\ell = -1$ that $(\lambda/\mu)^{2\ell} = 1$, hence k is a finite even integer, and ℓ is an odd multiple of $k/2$. □

We are now ready to write down the conclusion for the case $s = 1$.

Theorem 3.16. *Let K be a field of characteristic different from 2, and $k > 1$ be an integer. There exists a 0-bijection $f(x) = (x+1)/(tx+1)$ of finite 0-order k, for some $t \in K$ if and only if k is odd and one of the following three conditions is satisfied:*

- *k is equal to the characteristic of K;*
- *a primitive k-th root of unity lies in K;*
- *a primitive k-th root of unity is an element of norm 1 in a quadratic extension of K.*

In particular, if K is the finite field $\mathbb{F}_q$, for $q = p^n$, then such a 0-bijection exists if and only if k is odd and

- $k = p$
- *or* $k \mid (q-1)$,
- *or* $k \mid (q+1)$.

Proof. The fact that k has to be odd was proved in Lemma 3.15. The case $t = 0$ was studied in Proposition 3.3 and corresponds to the case $k = \mathrm{char}(K)$ (if not 0). The other cases, including the explicit construction of t, were established in Theorem 3.12. The reformulation for the finite field case results from Proposition 3.6. □

4 Orders of mappings in $\mathbb{Z}/n\mathbb{Z}$

Our main task is to describe the behaviour of the mappings $f_{s,t}$ on rings $\mathbb{Z}/n\mathbb{Z}$. Again, we shall consider n to be odd.

As in the field case, we study first the projective version of the mapping $f_{s,t} = \frac{sx+1}{tx+1}$ and compute its projective 0-order. Secondly, we determine whether this projective mapping meets infinity or not. Before we can proceed, we need to adapt the definitions.

Let R be a commutative ring. We denote by R^* the multiplicative group of invertible elements of R. This group acts componentwise on R^2. If $(a, b) \in R^2$ is such that the ideal $aR + bR$ is equal to R, then the same is true for the ideal $uaR + ubR$ when $u \in R^*$. This allows the definition of the projective line :

$$\mathbb{P}^1(R) = \{(a, b) \in R^2, aR + bR = R\}/R^* .$$

The group $G_2(R)$ of 2×2 matrices $F = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with invertible determinant $(ad - bc) \in R^*$ acts on $\mathbb{P}^1(R)$ by the classical formulae. Its elements define automorphisms of $\mathbb{P}^1(R)$. This is in particular the case for $F_{s,t} = \left(\begin{smallmatrix} s & 1 \\ t & 1 \end{smallmatrix}\right)$ when

$$(s - t) \in R^* .$$

We also define its characteristic polynomial $P_{s,t} = x^2 - (s+1)x + s - t$ with discriminant $D_{s,t} = (s-1)^2 + 4t$, exactly as in Section 3.

Definition 4.1. Let F be an automorphism of the projective line $\mathbb{P}^1(R)$. We say that F is of *projective 0-order k* if k is the smallest positive integer such that $F^k\binom{0}{1} = \binom{0}{x}$, for some $x \in R^*$.
We say that F *meets infinity* at ℓ, if $F^\ell\binom{0}{1} = \binom{x}{y}$, for some $(x, y) \in R^2$, $y \notin R^*$. We say simply that F meets infinity if there is some ℓ at which it happens.
We say that F is of *0-order k* if F is of projective 0-order k and never meets infinity.

When R is a field, all these definitions coincide with those defined in Section 3.

As in the field case, it is immediate from the definition that a mapping $f_{s,t}$ is of 0-order k if and only if the corresponding automorphism $F_{s,t}$ is of 0-order k.

The work is already done in the case $\mathbb{Z}/p\mathbb{Z}$, for p prime, at least when $s = 1$. This knowledge, of course, is useful when studying $\mathbb{Z}/n\mathbb{Z}$ in general. There are two cases to be considered, one of which is very easy.

Proposition 4.1. *Let $R = \mathbb{Z}/mn\mathbb{Z}$, where m and n are coprime, and let $s \in R$. Then there exists some $t \in R$ with $s - t \in R^*$ such that $f_{s,t}$ is of 0-order k if and only if the reduction modulo m of $f_{s,t}$ is of 0-order k_1 in $\mathbb{Z}/m\mathbb{Z}$, the reduction modulo n of $f_{s,t}$ is of 0-order k_2 in $\mathbb{Z}/n\mathbb{Z}$, and k is the least common multiple of k_1 and k_2.*

Proof. Use the Chinese remainder theorem. □

The other case requires more work and concerns the ring $R = \mathbb{Z}/p^r\mathbb{Z}$, for p prime. In this context, the condition $s - t \in R^*$ is equivalent to $s \not\equiv t \pmod{p}$.

We consider first the situation when $D_{s,t} \equiv 0 \pmod{p}$, and generalize Proposition 3.3 in Proposition 4.3. Before this, we need a lemma.

Lemma 4.2. *Let A and B be 2×2 matrices, with coefficients in $\mathbb{Z}$. Let p be a prime number and $\alpha \geq 1$ be an integer. If $A \equiv B \pmod{p^\alpha}$ and $B \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod{p}$, then $A^p \equiv B^p \pmod{p^{\alpha+1}}$.*

Proof. Let C be the matrix with integer coefficients such that $A = B + p^\alpha C$. Expanding the product, we find $A^p \equiv B^p + p^\alpha(B^{p-1}C + B^{p-2}CB + \cdots + CB^{p-1}) \pmod{p^{\alpha+1}}$. The condition $B \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod{p}$ implies that the sum in brackets is $B^{p-1}C + B^{p-2}CB + \cdots + CB^{p-1} \equiv pC \equiv 0 \pmod{p}$, and we get $A^p \equiv B^p \pmod{p^{\alpha+1}}$. □

Proposition 4.3. *Let s and t be elements of the ring $R = \mathbb{Z}/p^r\mathbb{Z}$, such that $s \not\equiv t \pmod{p}$. If $D_{s,t} \equiv 0 \pmod{p}$, then the projective 0-order of $F_{s,t}$ is equal to*

$$k = \begin{cases} p^r & \text{if } p \geq 5 \\ p^{r-q+1} & \text{if } p = 3 \text{ and } q = v_3(D_{s,t} + 3(s-t)) \end{cases}$$

If furthermore $s \equiv 1 \pmod{p}$ (in which case the condition $D_{s,t} \equiv 0 \pmod{p}$ simplifies to $t \equiv 0 \pmod{p}$), then $F_{s,t}$ does not meet infinity.

Remark 4.4. *We use here the notation $v_3(x)$ for the valuation at the prime 3. Since it is evaluated at elements of $\mathbb{Z}/3^r\mathbb{Z}$, this valuation is always bounded by r, including at 0.*

Proof. We can assume that $r \geq 2$, since the case $r = 1$ is contained in Proposition 3.3. The condition $D \equiv 0 \pmod{p}$ implies that we can write $t = -\left(\frac{s-1}{2}\right)^2 + pa$ for some a defined modulo p^{r-1}. We have $s - t = s + \left(\frac{s-1}{2}\right)^2 - pa = \left(\frac{s+1}{2}\right)^2 - pa$, hence $u = \frac{s+1}{2}$ is invertible. With the notation $N = \left(\begin{smallmatrix} (s-1)/2 & 1 \\ -(s-1)^2/4 & -(s-1)/2 \end{smallmatrix}\right)$ and $A = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$, we have $F = uI + N + paA$, where $B = N + paA$ satisfies $B^2 = paI$.

For the next argument, we have to separate the cases $p \geq 5$ and $p = 3$.

Consider first the case $p \geq 5$. For $i \geq 4$, we have $B^i \equiv 0 \pmod{p^2}$, hence

$$\begin{aligned} F^p &\equiv u^pI + pu^{p-1}B + \tfrac{p(p-1)}{2}u^{p-2}B^2 + \tfrac{p(p-1)(p-2)}{6}u^{p-3}B^3 && \pmod{p^2} \\ &\equiv \left(u^p + \tfrac{ap^2(p-1)}{2}u^{p-2}\right)I + \left(pu^{p-1} + \tfrac{ap^2(p-1)(p-2)}{6}u^{p-3}\right)B && \pmod{p^2} \\ &\equiv u^pI + \left(pu^{p-1} + \tfrac{ap^2(p-1)(p-2)}{6}u^{p-3}\right)B && \pmod{p^2} \end{aligned}$$

Since $p \geq 5$, the coefficient $\frac{ap^2(p-1)(p-2)}{6}$ is divisible by p^2 and the expression simplifies to

$$\begin{aligned} F^p &\equiv u^pI + pu^{p-1}B && \pmod{p^2} \\ &\equiv u^pI + pu^{p-1}N && \pmod{p^2} \end{aligned}$$

This relation can be written as $F^p \equiv vI + p^qwN \pmod{p^{q+1}}$, where $v = u^p$ and $w = u^{p-1}$ are invertible, and $q = 1$.

If $p = 3$, we have $F^3 = u^3I + 3u^2B + 3uB^2 + B^3 = (u^3 + 9au)I + 3(u^2 + a)B$, where $u^3 + 9au$ is invertible since u is invertible. By definition, we have $q = v_3(D_{s,t} + 3(s-t)) = v_3(3(u^2 + a))$. If $q = r$, we have directly $F^3 = (u^3 + 9au)I$ and we get the conclusion that the projective 0-order of F is 3. If $q < r$, we can write

$$F^3 \equiv (u^3 + 9au)I + 3(u^2 + a)N \pmod{p^{q+1}}.$$

or $F^p \equiv vI + p^qwN \pmod{p^{q+1}}$, where v and w are invertible.

We have now exactly the same relations is both cases $p \geq 5$ and $p = 3$, and we can finish the proof with a common argument. The coefficient v is invertible, so that we can apply Lemma 4.2 to $v^{-1}F^p$ and get by induction

$$\begin{aligned} F^{p^\alpha} &\equiv (vI + p^v wN)^{p^{\alpha-1}} && \pmod{p^{q+\alpha}} \\ &\equiv v^{p^{\alpha-1}} I + p^{q+\alpha-1} wN && \pmod{p^{q+\alpha}} \end{aligned}$$

for all $1 \leq \alpha \leq r - q + 1$. For $\alpha = r - q$, this gives $F^{p^{r-q}}\binom{0}{1} = v^{p^{r-q-1}}\binom{0}{1} + p^{r-1}w\binom{1}{-(s-1)/2}$. Inspecting the first coefficient reveals that the projective 0-order of F is not a divisor of p^{r-q}. For $\alpha = r - q + 1$, this gives $F^{p^{r-q+1}}\binom{0}{1} = v^{p^{r-q}}\binom{0}{1}$, hence the projective 0-order of F is exactly p^{r-q+1}, as claimed.

So far we considered the projective 0-order and not the 0-order itself. It remains to determine whether $F_{s,t}$ meets infinity. By definition, $F_{s,t}$ meets infinity at ℓ if the reduction modulo p of $F_{s,t}$ meets infinity at ℓ. When $s \equiv 1 \pmod{p}$, Proposition 3.3 says that the reduction modulo p of $F_{s,t}$ does not meet infinity, hence $F_{s,t}$ does not meet infinity at all. □

Hence the case $D_{s,t} \equiv 0 \pmod{p}$ is finished and we can focus on the case when $D_{s,t} \not\equiv 0 \pmod{p}$.

We first suppose that $D_{s,t}$ is an invertible square in R, or equivalently that it is a nonzero square modulo p.

Proposition 4.5. *Let $R = \mathbb{Z}/p^r\mathbb{Z}$*

- *Let s, t be elements of R with $s \not\equiv t \pmod{p}$. If $D_{s,t}$ is a nonzero square modulo p, then the projective 0-order of $F_{s,t}$ is of the form $k = k'p^m$ where $m < r$ and k' is the projective 0-order of the reduction modulo p of $F_{s,t}$. In particular, k' satisfies $1 < k' \mid (p-1)$.*
  If furthermore $s \equiv 1 \pmod{p}$ (and t is a nonzero square modulo p) then $F_{s,t}$ meets infinity if and only if k is even.
- *Let s be an element of R with $s \not\equiv -1 \pmod{p}$, and $k = k'p^m$ be an integer with $m < r$ and $2 < k' \mid (p-1)$. There exist exactly $\varphi(k)/2$ choices of $t \in R$, $t \not\equiv s \pmod{p}$, such that $F_{s,t}$ is of projective 0-order k.*

Proof. Consider the first part of the proposition, and let s and t be as required. We can apply the results of the section to the reduction of F modulo p. In particular, since $D \not\equiv 0 \pmod{p}$, there exist exactly two distinct roots λ_p and μ_p of the characteristic polynomial P modulo p. They satisfy $\lambda_p\mu_p \equiv s - t \pmod{p}$, hence λ_p and μ_p are invertible. Since p is odd, an application of Hensel's Lemma implies that D is in fact a square in $\mathbb{Z}/p^r\mathbb{Z}$ and that there exist exactly two distinct elements λ and μ of $\mathbb{Z}/p^r\mathbb{Z}$ such that $P(\lambda) = P(\mu) = 0$. These elements satisfy furthermore $\lambda \equiv \lambda_p \pmod{p}$ and $\mu \equiv \mu_p \pmod{p}$, and also the relation $\lambda\mu = s - t$, hence are both invertible. Another useful relation is $(\lambda - \mu)^2 = D$, hence $\lambda - \mu$ is also invertible.

The expression of $F^i\binom{0}{1}$ in terms of λ, μ and i given in Proposition 3.4 still applies in our context. Inspecting its first coefficient implies that the projective 0-order of F is again the multiplicative order of the invertible element λ/μ, or equivalently the smallest positive integer k such that $(\lambda/\mu)^k = 1$.

Now, the group $(\mathbb{Z}/p^r\mathbb{Z})^*$ is cyclic of order $(p-1)p^{r-1}$, hence the projective 0-order k of F is $k = k'p^m$ with $k' \mid (p-1)$ and $m < r$. More precisely, we have an isomorphism of groups:

$$\phi : (\mathbb{Z}/p^r\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{r-1}\mathbb{Z}$$

(the group on the left is multiplicative and the groups on the right are additive). The first coordinate of ϕ in $\mathbb{Z}/(p-1)\mathbb{Z}$ is given by the reduction modulo p followed by the isomorphism $(\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$. This isomorphism shows that k' is equal to multiplicative order of λ_p/μ_p in $(\mathbb{Z}/p\mathbb{Z})^*$, that is by the projective 0-order of the reduction of F modulo p according to Proposition 3.4.

When $s \equiv 1 \pmod{p}$, we can apply Lemma 3.15 and deduce that F meets infinity modulo p if and only if k' is even, hence also in R.

Consider now the second part of the proposition and let s and k be as required. Using the isomorphism ϕ, we see that there are exactly $\varphi(k)$ choices of $\zeta \in R^*$ that are of multiplicative order exactly k. Since $k' > 2$, we have $\zeta \not\equiv -1 \pmod{p}$, hence $\zeta + 1$ is invertible. The rest of the proof is

analogous to the proof of Proposition 3.7. In particular, the value of t is given by the same formula $t = \frac{(\zeta-s)(s\zeta-1)}{(\zeta+1)^2}$. □

The case when $D_{s,t}$ is an invertible nonsquare in R (or equivalently when it is not a square modulo p) is similar but technically less transparent. Exactly as in the case of fields where the eigenvalues were found in a quadratic extension, we need to build a quadratic extension of R containing the eigenvalues.

Proposition 4.6. *Let $R = \mathbb{Z}/p^r\mathbb{Z}$*

- *Let s, t be elements of R with $s \not\equiv t \pmod p$. If $D_{s,t}$ is not a square modulo p, then the projective 0-order of $F_{s,t}$ is of the form $k = k'p^m$ where $m < r$ and k' is the projective 0-order of the reduction modulo p of $F_{s,t}$. In particular, k' satisfies $1 < k' \mid (p+1)$.*
  If furthermore $s \equiv 1 \pmod p$ (and t is not a square modulo p) then $F_{s,t}$ meets infinity if and only if k is even.
- *Let s be an element of R with $s \not\equiv -1 \pmod p$, and $k = k'p^m$ be an integer with $m < r$ and $2 < k' \mid (p+1)$. There exist exactly $\varphi(k)/2$ choices of $t \in R$, $t \not\equiv s \pmod p$, such that $F_{s,t}$ is of projective 0-order k.*

Proof. Let $d \in \mathbb{Z}$ be an integer which is not a square modulo p. We consider the quadratic field $L = \mathbb{Q}(\sqrt{d})$ and $\mathcal{O}$ its ring of integers. By construction the polynomial $x^2 - d$ is irreducible modulo p, hence the ideal $p\mathcal{O}$ is a prime ideal of $\mathcal{O}$ (see [3, §4.8] for more justification). In particular, $\mathcal{O}/p\mathcal{O}$ is a finite field with p^2 elements and the ring $R' = \mathcal{O}/p^r\mathcal{O}$ contains a copy of R. There are group isomorphisms

$$(\mathcal{O}/p\mathcal{O})^* \;\cong\; \mathbb{Z}/(p^2-1)\mathbb{Z}$$

and

$$(\mathcal{O}/p^r\mathcal{O})^* \;\cong\; (\mathcal{O}/p\mathcal{O})^* \times \mathcal{O}/p^{r-1}\mathcal{O} \;\cong\; \mathbb{Z}/(p^2-1)\mathbb{Z} \times (\mathbb{Z}/p^{r-1}\mathbb{Z})^2 \,.$$

The first one is the well known fact that the multiplicative group of a finite field is cyclic and the second one is proved in [4, Prop 4.2.4 and 4.2.8].

Let us now come to the proof of the first part of the proposition, and let s and t be elements as required. We can use exactly the same argument as for the previous proposition: the reduction of the characteristic polynomial P has exactly two distinct roots λ_p and μ_p in $\mathcal{O}/p\mathcal{O}$, and by a Hensel's lifting, P has exactly two distinct roots λ and μ in R'. We can then use the formula of Proposition 3.4 and deduce that the projective 0-order of F is the multiplicative order of λ/μ in $(\mathcal{O}/p^r\mathcal{O})^*$. Using the isomorphism, we deduce that this order is of the form $k = k'p^m$ with $m < r$ and $k' \mid (p^2-1)$. But we also deduce that k' is the projective 0-order of the reduction modulo p of F, hence, according to the results of section , is a divisor of $p+1$.

When $s \equiv 1 \pmod p$, we can apply Lemma 3.15 and deduce that F meets infinity modulo p if and only if k' is even, hence also in R.

For the second part of the proposition, let s and k be as required. Following the same proof as for Proposition 4.5, we see that there are exactly $\varphi(k)$ choices of $\zeta \in R'^*$ that are of multiplicative order exactly k, and exactly $\varphi(k)/2$ choices of $t \in R'$, given by the formula $t = \frac{(\zeta-s)(s\zeta-1)}{(\zeta+1)^2}$, such that $F_{s,t}$ is of projective 0-order k. It remains to prove that t is indeed in R and not only in R'.

The norm map from $\mathcal{Q}(\sqrt{d})$ to $\mathcal{Q}$ sends $p^r\mathcal{O}$ to $p^r\mathbb{Z}$, and defines another norm map from R'^* to R^*, which is a group homomorphism. Its image contains trivially all the squares of R^* as the norm of elements of R^*, but also contains $d = \mathrm{norm}(\sqrt{d})$. Hence the norm is surjective and its kernel is a subgroup of R'^* of order $(p+1)p^{r-1}$. From this, we see that the elements of order $p+1$ in R'^* have norm 1. Now, the same proof as for Proposition 3.10 will again give the conclusion that $t \in R$. □

Hence we can conclude what happens for any $\mathbb{Z}/n\mathbb{Z}$ if $s = 1$.

Theorem 4.7. *Let $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_m^{r_m}$ be the prime factorization of a positive odd number and let $k > 1$ be an integer. Then there exists $t \in \mathbb{Z}/n\mathbb{Z}$ such that $f_{1,t}$ is a 0-bijection from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ of 0-order k if and only if k is odd and there exist $k_1, \ldots, k_m$ and $\varepsilon_1, \ldots, \varepsilon_m$ satisfying the three conditions:*

- *$\varepsilon_i \in \{-1, 0, 1\}$, $k_i = k_i' p^{e_i}$, where $2 < k_i' \mid (p_i + \varepsilon_i)$ and $e_i < r_i$, for all $1 \le i \le m$;*

- *if $\varepsilon_i = 0$ and $p_i > 3$, for some i, then $k_i = p_i^{r_i}$;*
- *the least common multiple of $k_1, \dots, k_m$ is k.*

Proof. We make an induction on m. Suppose first that $m = 1$. We have seen in Lemma 3.15 that $F_{1,t}$, for $t \not\equiv 0 \pmod p$, meets infinity if and only if its projective order is even. But if $t \equiv 0 \pmod p$ then k_1 is a divisor of $p_1^{r_1}$, according to Proposition 4.3. Hence k has to be odd.

The previous three propositions ensure that the theorem holds in the case of $m = 1$. The induction step can be done using Proposition 4.1. □

5 The question of isomorphism

From now on, we shall consider the case $s = 1$ only. We know already when there exists an appropriate fractional mapping of 0-order k on R, in the case when R is a field or a quotient of $\mathbb{Z}$. Nevertheless, we do not know still if different choices of t, that lead to the same k, give raise to different A-loops or not. The answer depends on the ring. For fields and $\mathbb{Z}/p^r\mathbb{Z}$ there exist a unique loop for each admissible 0-order. In the other cases there can be more isomorphism classes. We shall ignore the case $t = 0$ since the associated loop is a group then, according to Proposition 2.3.

From now on, R is either a field or $\mathbb{Z}/n\mathbb{Z}$. We are in a special case, namely $s = 1$, hence some things that we have already established simplify substantially. It is useful to have a description of what elements can be obtained as $f^i(0)$.

Lemma 5.1. *Let $t \in R^*$ be such that $t - 1 \in R^*$ and $f_{1,t}$ is of finite 0-order k. Then $k > 2$ and*

(i) $t = \left(\frac{\zeta-1}{\zeta+1}\right)^2$ *where ζ is an element of multiplicative order k (in an extension of R).*

(ii) *The roots of the characteristic polynomial are $\lambda = \frac{2\zeta}{\zeta+1}$ and $\mu = \frac{2}{\zeta+1}$.*

(iii) $F_{1,t}^i\binom{0}{1} = \begin{pmatrix} \frac{\lambda^i-\mu^i}{\lambda-\mu} \\ \frac{\lambda^i+\mu^i}{2} \end{pmatrix}$

(iv) $f_{1,t}^i(0) = \dfrac{\zeta+1}{\zeta-1} \cdot \dfrac{\zeta^i-1}{\zeta^i+1}$

Proof. (i) was stated in Proposition 3.12 for fields; for $R = \mathbb{Z}/p^r\mathbb{Z}$ it is the same according to the proofs of Proposition 4.5 or 4.6. In the case of $\mathbb{Z}/mn\mathbb{Z}$, for m and n coprime, we use induction and the Chinese remainder theorem.

For proving (ii) just check that $\lambda + \mu = 2$ and $\lambda\mu = 1 - t$.

(iii) Something similar was written in Proposition 3.4 with the exception that the second coordinate was $\frac{\lambda^i(1-\mu)-\mu^i(1-\lambda)}{\lambda-\mu}$. But $\frac{1-\mu}{\lambda-\mu} = \frac{\zeta+1-2}{\zeta+1} \cdot \frac{\zeta+1}{2\zeta-2} = \frac{1}{2}$ and analogously $\frac{1-\lambda}{\lambda-\mu} = -\frac{1}{2}$. Hence the second coordinate simplifies to $(\lambda^i + \mu^i)/2$.

(iv) By (iii), we have $f_{1,t}^i(0) = \frac{\lambda^i-\mu^i}{\lambda-\mu} \cdot \frac{2}{\lambda^i+\mu^i}$. Replacing 2 by $\lambda + \mu$ and using the relation $\frac{\lambda}{\mu} = \zeta$, we get $f_{1,t}^i(0) = \frac{\zeta^i-1}{\zeta-1} \cdot \frac{\zeta+1}{\zeta^i+1}$. □

As a byproduct, we can rewrite Proposition 2.1 in a better looking way, at least for the case $t \in R^*$.

Proposition 5.2. *Let M be a module over a ring R, which is either a field or the ring $\mathbb{Z}/n\mathbb{Z}$. Suppose that there exists ζ, an element of an odd order k, lying either in R^*, or in a quadratic extension of R and being of norm 1, with respect to R. Then we can define a commutative A-loop on the set $M \times \mathbb{Z}/k\mathbb{Z}$ as follows:*

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

This loop is equal to $M[1, t]$ for $t = \left(\frac{\zeta-1}{\zeta+1}\right)^2$.

Proof. It was described in Theorem 3.16 and Theorem 4.7 that for the specified choices of k there exists a t such that $f_{1,t}$ is of 0-order k. According to Lemma 5.1, we have $t = \left(\frac{\zeta-1}{\zeta+1}\right)^2$ and $f^i(0) = \frac{\zeta+1}{\zeta-1} \cdot \frac{\zeta^i-1}{\zeta^i+1}$. Hence $1 + tf^i(0)f^j(0) = \frac{2(\zeta^{i+j}+1)}{(\zeta^i+1)(\zeta^j+1)}$ and we insert this expression into Proposition 2.1. □

We are ready now to tackle the problem of isomorphism. We shall use the result Drápal found when studying his construction.

Proposition 5.3 (Drápal [5])**.** *Let M be a faithful module over a commutative ring R. Let $t, t' \in R^*$ be of the same finite 0-order k. Then an isomorphism $M[1,t] \cong M[1,t']$ which restricts to the identity upon $M \times \{0\}$ exists if and only if $t' = td^2$ for some $d = f^r(0)$, where $1 \leq r < k$, $r \in \mathbb{Z}_k^*$. This condition is necessary and sufficient when $M(+)$ is a cyclic group.*

We already know what elements can be $f^r(0)$ and hence we can give an immediate answer: the construction is unique in the case of invertible elements in a field or in $\mathbb{Z}/p^r\mathbb{Z}$.

Proposition 5.4. *Let M be a faithful module over R, which is either a field or $\mathbb{Z}/p^r\mathbb{Z}$. Let $t, t' \in R^*$ be of the same finite 0-order k. Then the loops $M[1,t]$ and $M[1,t']$ are isomorphic.*

Proof. Write $t = \left(\frac{\zeta-1}{\zeta+1}\right)^2$ and $t' = \left(\frac{\zeta'-1}{\zeta'+1}\right)^2$. The element ζ is of multiplicative order k in R^* and so is the element ζ'. Since all k-th roots of 1 belong to the cyclic group generated by ζ, there exists some i such that $\zeta' = \zeta^i$.

According to Lemma 5.1 we have $f^i(0) = \frac{\zeta+1}{\zeta-1} \cdot \frac{\zeta^i-1}{\zeta^i+1}$ which is the d we are looking for. Indeed,

$$td^2 = \left(\frac{\zeta-1}{\zeta+1}\right)^2 \cdot \left(\frac{\zeta+1}{\zeta-1} \cdot \frac{\zeta^i-1}{\zeta^i+1}\right)^2 = \left(\frac{\zeta'-1}{\zeta'+1}\right)^2 = t'$$

Now the conditions of Proposition 5.3 are fulfilled. □

The uniqueness does not hold in the general case; the smallest examples, brought by the following proposition, are two non-isomorphic loops of order $5 \cdot 11 \cdot 19$.

Proposition 5.5. *Let $R = \mathbb{Z}/pq\mathbb{Z}$, where p and q are distinct primes. Let and odd $k > 2$ divide either $p-1$ or $p+1$ as well as either $q-1$ or $q+1$. Then there exist exactly $\varphi(k)/2$ non-isomorphic loops of order kpq, obtained as $R[1,t]$ for some $t \in R^*$.*

Proof. We have $R \cong \mathbb{F}_p \times \mathbb{F}_q$. A mapping F is of 0-order k on R if and only if both projections are of 0 order k on R. There exist exactly $\varphi(k)/2$ choices of such a t_p in $\mathbb{F}_p$ and there exist exactly $\varphi(k)/2$ choices of such a t_q in $\mathbb{F}_q$, thus giving $\varphi(k)^2/4$ choices of $t = (t_p, t_q)$.

We have $t_p = (\zeta_p - 1)/(\zeta_p + 1)$ where ζ_p is a primitive k-th root of 1 in $\mathbb{F}_p$. But $t_p = (\zeta_p^{-1} - 1)/(\zeta_p^{-1} + 1)$ too and these are both possibilities how to obtain t_p from a primitive k-th root of 1 in $\mathbb{F}_p$. The same holds for t_q and therefore there are four possibilities how to obtain t, namely from (ζ_p, ζ_q), (ζ_p, ζ_q^{-1}), (ζ_p^{-1}, ζ_q) and $(\zeta_p^{-1}, \zeta_q^{-1})$.

Now we follow the proof of Proposition 5.4. The cyclic group generated by (ζ_p, ζ_q) has $\varphi(k)$ elements; they give raise to $\varphi(k)/2$ different values of t' since (ζ_p^i, ζ_q^i) gives the same t' as $(\zeta_p^{-i}, \zeta_q^{-i})$. The elements from the cyclic subgroup generated by (ζ_p, ζ_q^{-1}) follow the structure of the subgroup generated by (ζ_p, ζ_q), meaning that the first coordinate is the same and the second is inverted, and therefore the same values of t' are obtained. Hence, according to Proposition 5.3, one loop with a given t is isomorphic to exactly $\varphi(k)/2$ loops $R[1,t']$ (including itself).

We know that there are $\varphi(k)^2/4$ choices of t which are split into isomorphism classes of $\varphi(k)/2$ elements. Hence there are $\varphi(k)/2$ isomorphism classes. □

We do not give any result for $t \notin R^*$ since the article of Drápal does not give us a tool for studying it. Nevertheless, it seems that something similar to Proposition 5.3 is true here: a computer computation using the GAP package Loops [9] gives $\mathbb{Z}/25\mathbb{Z}[1,5] \cong \mathbb{Z}/25\mathbb{Z}[1,20] \ncong \mathbb{Z}/25\mathbb{Z}[1,10] \cong \mathbb{Z}/25\mathbb{Z}[1,15]$. In other words, they are isomorphic if and only if t and t' differ by a square. Another example is $\mathbb{Z}/27\mathbb{Z}[1,6] \ncong \mathbb{Z}/27\mathbb{Z}[1,15]$ to see that it concerns 3-loops too.

A different question is whether, given a $t \in \mathbb{F}_p^*$, there is an isomorphism between $\mathbb{F}_{p^r}[1,t]$ and $\mathbb{Z}/p^r\mathbb{Z}[1,t]$. The answer is easy there: according to Proposition 2.1, we have $\mathrm{Inn}(\mathbb{F}_{p^r}[1,t]) \cong \mathbb{Z}/p^r\mathbb{Z} \rtimes \mathbb{Z}/(p-1)\mathbb{Z}$ and $\mathrm{Inn}(\mathbb{Z}/p^r\mathbb{Z}[1,t]) \cong \mathbb{Z}/p^r\mathbb{Z} \rtimes \mathbb{Z}/p^{r-1}(p-1)\mathbb{Z}$. Hence the loops cannot be isomorphic.

6 Loops of a semiprime order

The first motivation when writing this article was to describe all commutative A-loops of order kp, for k and p primes (not necessarily distinct). The first half of this section deals with this question; the work is nearly completed up to one result which is expected to appear soon.

Any construction of commutative A-loops of an odd order is helpful when studying Bruck loops too: Kinyon, Vojtěchovský and the first author proved in [6] that when $(Q,\cdot)$ is a non-associative commutative A-loop of an odd order then there exists an operation $\circ$ on Q defined by

$$x \circ y = (x \cdot y^2/x^{-1})^{\frac{1}{2}}$$

such that $(Q,\circ)$ is a non-associative Bruck loop. In the second half of the section we give the explicit formula for the Bruck loop that arises this way from the commutative A-loops studied here.

But first we look at commutative A-loops of order kp.

Theorem 6.1. *Let $k \leq p$ be two primes. Then there exists a non-associative commutative A-loop of order kp if and only if $k > 2$ and k divides $p^2 - 1$.*

Proof. "If": Let ζ be a primitive k-th root of 1 within $\mathbb{F}_{p^2}$ and put $t = \left(\frac{\zeta-1}{\zeta+1}\right)^2$. Then $\mathbb{Z}_p[1,t]$ is a commutative A-loop of order kp, according to Lemma 5.1 and Proposition 2.4. It is not associative according to Proposition 2.3.

"Only if": It was proved in [7] that commutative A-loops of orders $2p$ and p^2 are groups. Hence we can suppose $2 < k < p$. It was already said, in the beginning of the section, that once $(Q,\cdot)$ is an odd order commutative A-loop, there exists a non-associative Bruck loop of the same cardinality, namely $(Q,\circ)$. And according to Sharma [11], there exists a non-associative Bruck loop of order kp, for such k and p, if and only if k divides $p^2 - 1$. □

It is highly probable that such a loop is unique.

Conjecture 6.2. *Let k and p be two primes. Then there exists at most one non-associative commutative A-loop of order kp, up to isomorphism.*

Idea of a proof: Aleš Drápal has a continuing programme to classify all loops with metacyclic inner mapping groups and trivial centers. It turned out that these loops fall into six types of constructions. The construction described in Proposition 2.1 is the only one of them yielding commutative A-loops.

It was proved in [7] that a commutative A-loop of order kp must have a trivial center and a normal subloop of order p. From this, it is easy to prove that such a loop must have a metacyclic inner mapping group. Hence it must fall into one of the categories described by Drápal and that means that it must be achievable by the construction of this paper. And, according to Proposition 5.4, all constructed loops of order kp are isomorphic.

The reason why this proof cannot be considered complete is that the results of Drápal programme have not been written yet, and thus cannot be independently verified. □

Now we shall concentrate on the Bruck loops associated to our commutative A-loops.

Theorem 6.3. *Let M be a module over a ring R, which is either a field or the ring $\mathbb{Z}/n\mathbb{Z}$. Suppose that there exists ζ, an element of an odd order k, lying either in R^*, or in a quadratic extension of R and being of norm 1, with respect to R. Then we can define a loop on the set $M \times \mathbb{Z}/k\mathbb{Z}$ as follows:*

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

This loop is a Bruck loop.

Proof. The proof is a straightforward calculation. In the beginning of the section we explained how to associate a Bruck loop to an odd order commutative A-loop. Here we compute the operation $\circ$ associated to the operation $\cdot$ given in Proposition 5.2. We see immediately that $(a,i)^{-1} = (-a,-i)$ and $(a,i)/(b,j) = \left(a \cdot \frac{2(\zeta^i+1)}{(\zeta^{i-j}+1)(\zeta^j+1)} - b, i-j\right)$. The element $(a,i)^{\frac{1}{2}}$ is the only element (b,j) such that $(b,j)^2 = (a,i)$. It is again easy to check $(a,i)^{\frac{1}{2}} = \left(a \cdot \frac{\zeta^i+1}{(\zeta^{\frac{j}{2}}+1)^2}, \frac{i}{2}\right)$. Hence we can compute $(a,i) \circ (b,j) = (((a,i)\cdot(b,j)^2)/(-a,-i))^{\frac{1}{2}}$ which eventually gives the expression from the theorem. □

Some Bruck loops of order kp were presented in [10]. It is not difficult to show that the Bruck loops constructed there are the same as the loops given in Theorem 6.3 for $R = \mathbb{F}_p$. However, our construction is explicit while the construction in [10] needed some recursive sequences to be found first.

In fact, these Bruck loops are the only known Bruck loops of order kp. It is conjectured that there exist no more such Bruck loops than these. One possible way to prove it is using the correspondence between commutative A-loops and Bruck loops together with Conjecture 6.2. But we still do not know whether this correspondence is a bijection.

Open Question 6.4. *The correspondence $(Q,\cdot) \mapsto (Q,\circ)$ is a correspondence between the class of all commutative A-loops of odd order and the class of all Bruck loops of odd order. Is this correspondence injective or surjective?*

References

[1] R. H. Bruck: *A survey of binary systems*, 3rd corrected printing, Ergebnisse der Mathematik und Ihrer Grenzgebiete, new series, volume **20**, Springer-Verlag (1971).

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

[3] H. Cohen: *A Course in Computational Algebraic Number Theory*, 4th corrected printing, GTM **138**, Springer-Verlag (2000).

[4] H. Cohen: *Advanced Topics in Computational Algebraic Number Theory*, GTM **193**, Springer-Verlag (1999).

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

[6] P. Jedlička, M. Kinyon, P. Vojtěchovský: *Structure of commutative automorphic loops*, Trans. of AMS **363**,1 (2011), 365–384

[7] P. Jedlička, M. Kinyon, P. Vojtěchovský: *Constructions of commutative automorphic loops*, Commun. in Alg. **38**, 9 (2010), 3243–3267

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

[9] G. Nagy, P. Vojtěchovský: *LOOPS: Computing with quasigroups and loops*, version 2.1.0, package for GAP, `http://www.math.du.edu/loops` .

[10] H. Niederreiter, K. H. Robinson: *Bol loops of order pq*, Math. Proc. Cambridge Philos. Soc., **89** (1981), 241–256.

[11] B. L. Sharma: *Bol loops of order pq with $q \mid (p^2-1)$*, Bolletino della Unione matematica italiana **1**,2 (1987), 163–169.

6 Nuclear semidirect product of commutative automorphic loops

Jan Hora, Přemysl Jedlička

Abstract

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

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

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

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

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

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

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

1 Analysis of the semidirect product

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

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

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

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

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

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

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

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

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

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

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

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

Turning back to the semidirect product: a semidirect product of groups is described by a mapping $\varphi : H \to \mathrm{Aut}(K)$ and, in fact, each automorphism from $\mathrm{Im}\,\varphi$ is a restriction of an inner automorphism of $K \rtimes_\varphi H$, that means of a mapping $k \mapsto h^{-1}kh$. In the case of commutative automorphic loops, inner automorphisms come into play too.

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

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

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

$$(a + i) + (b + j) = ((a + i) + b) + j = ((i + a) + b) + j = (i + (a + b)) + j = ((a + b) + i) + j.$$

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

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

Proposition 1.4. *Let H and K be abelian groups and let us have a mapping $\varphi : H^2 \to \mathrm{Aut}(K)$. We define an operation $*$ on $Q = K \times H$ as follows:*

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

Let us denote $\varphi_{i,j,k} = \varphi_{i,j+k} \circ \varphi_{j,k}$. Then Q is a commutative A-loop if and only if the following properties hold:

$$\varphi_{i,j} = \varphi_{j,i} \tag{1}$$
$$\varphi_{0,i} = \mathrm{id}_K \tag{2}$$
$$\varphi_{i,j} \circ \varphi_{k,n} = \varphi_{k,n} \circ \varphi_{i,j} \tag{3}$$
$$\varphi_{i,j,k} = \varphi_{j,k,i} = \varphi_{k,i,j} \tag{4}$$
$$\varphi_{i,j+k} + \varphi_{j,i+k} + \varphi_{k,i+j} = \mathrm{id}_K + 2 \cdot \varphi_{i,j,k} \tag{5}$$

Moreover, $K \times 0$ is a normal subgroup of Q, $0 \times H$ is a subgroup of Q and $(K \times 0) \cap (0 \times H) = 0 \times 0$ and $(K \times 0) + (0 \times H) = Q$.

Q is associative if and only if $\varphi_{i,j} = \mathrm{id}_K$, for all $i, j \in H$. The nuclei are $N_\mu(Q) = K \times \{i \in H;\ \forall j \in H :\ \varphi_{i,j} = \mathrm{id}_K\}$ and $N_\lambda = \{a \in K;\ \forall j, k \in H :\ \varphi_{j,k}(a) = a\} \times \{i \in H;\ \forall j \in H :\ \varphi_{i,j} = \mathrm{id}_K\}$.

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

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

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

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

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

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

and

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

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

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

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

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

and in (7) we get

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

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

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

and then in (7) to get

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

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

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

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

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

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

while the other side is

$$\begin{aligned}
&\varphi_{i,j}(\varphi_{m,n}\varphi_{n,i}^{-1}(u + \varphi_{n,i}(v + a) + \varphi_{m,n}\varphi_{n,j}^{-1}(u + \varphi_{n,j}(v + b) - 2\varphi_{m,n}(u + v)\\
&\quad = \varphi_{m,n}(\varphi_{i,j}(\varphi_{n,i}^{-1}(u) + v + a + \varphi_{n,j}^{-1}(u) + v + b - 2u - 2v) = \varphi_{m,n}\varphi_{i,j}(\varphi_{n,i}^{-1}(u) + \varphi_{n,j}^{-1}(u) - 2u + a + b)
\end{aligned}$$

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

Now we compute the middle nucleus.

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

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

2 Known examples

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

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

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

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

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

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

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

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

is a commutative A-loop.

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

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

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

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

while the right hand side is

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

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

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

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

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

is a commutative A-loop.

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

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

3 Small cyclic normal subgroup

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$\gamma((a,i,j)*(b,k,l)) = \gamma(((\alpha(i+k)+1)mn(a+b), i+k, j+l)) = ((\alpha(i+k)+1)mn(a+b), i+j+k+l))$$
$$\gamma((a,i,j))*\gamma((b,k,l)) = (a,i+j)*(b,k+l) = ((\alpha(i+j,k+l)mn+1)(a+b), i+j+k+l)$$

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

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

Proposition 3.6. *Let $K = \mathbb{Z}_{mp^2}$, for some prime p, and let H be an elementary abelian p-group. Let us have two bilinear forms $\alpha_1, \alpha_2 : H^2 \to \mathbb{Z}_p$. Let Q_1 and Q_2 be two loops obtained via the construction in Proposition 3.4, using the forms α_1 resp. α_2. Then $Q_1 \cong Q_2$ if and only if α_1 and α_2 are equivalent.*

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

$$\gamma((a,i)*_1(b,j)) = \gamma(((\alpha_1(i,j)\cdot mp+1)\cdot(a+b), i+j)) = (((\alpha_1(i,j)\cdot mp+1)\cdot(a+b), \beta(i+j)))$$
$$\gamma(a,i)*_2\gamma(b,j) = (a,\beta(i))*_2(b,\beta(j)) = ((\alpha_2(\beta(i),\beta(j))mp+1)(a+b),$$
$$\beta(i)+\beta(j)) = (((\alpha_1(i,j)\cdot mp+1)\cdot(a+b), \beta(i+j)))$$

and γ is a homomorphism. The bijection is clear.

"⇒" Let α_1 and α_2 be nonequivalent symmetric bilinear forms. If the dimensions of the radicals of the forms α_i are not equal, we get, by Proposition 3.4, different sizes of middle nuclei and thus non-isomorphic corresponding loops. Thus we can assume that the dimensions of the radicals of the forms α_i are equal. Moreover, by Lemma 3.5 the loop is then a direct product of the radical and of a smaller loop. We can hence suppose that α_1 and α_2 are non-degenerate.

Let γ be an isomorphism $Q_1 \to Q_2$. Since α_1 and α_2 are non-degenerate, $N_\mu(Q_1) = N_\mu(Q_2) = K \times 0$. And therefore γ restricted on $K\times 0$ is an automorphism (we shall thus understand γ as an automorphism of K). On the other hand $\gamma(H) \neq H$ in general. Let us write $\gamma((0,i)) = (\delta(i),\beta(i))$, for $i, \beta(i) \in H$ and $\delta(i) \in K$. We thus have $\gamma((a,i)) = (\gamma(a),0)*_2(\delta(i),\beta(i)) = (\gamma(a)+\delta(i),\beta(i))$. Now

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

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

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

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

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

from which

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

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

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

and the bilinear forms are equivalent. □

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

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

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

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

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

Remark 3.8. *In the previous corollary all possible commutative A-loops were enumerated but no hint was given how to distinguish them structurally, especially those coming from non-degenerate forms. If p is odd and the dimension is $2k$, we get by Witt's theorem that the two non-equivalent forms differ in the dimension of (any) maximal isotropic subspace (usually called index or Witt index). One of the forms has index k and the other $k-1$ and thus the size of any maximal associative subloop of Q containing K differ for the two loops obtained by the construction. On the other hand, if the dimension is odd, the two non-equivalent forms are similar (one is a multiple of the other) and thus the structure of the corresponding loops is similar (see Example 3.9).*

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

$$((1, i) * (0, i)) * (0, i) = (\varphi_{i,i}(1), 0) * (0, i) = (\varphi_{i,i}(1), i),$$
$$(1, i) * ((0, i) * (0, i)) = (1, i) * (0, 0) = (1, i)$$

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

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

4 Bilinear mappings

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

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

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

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

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

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

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

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

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

- *there exists a generating subset $\{x_1, \dots, x_k\}$ of R such that $nx_i = 0$ and $x_i x_j = 0$, for all i, j;*
- *R is a commutative ring and there exists G, a subgroup of R^* generating R, such that, for all $a, b, c \in G$, we have $na = n$ and $ab + bc + ca = 1 + 2abc$.*

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

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

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

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

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

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

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

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

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

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

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

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

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

□

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

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

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

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

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

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

References

[1] D. A. S. de Barros, A. Grishkov, P. Vojtěchovský: *Commutative automorphic loops of order p^3*, J. Algebra Appl. **11**,5 (2012), 15 pages

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

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

[4] S. Gagola III: *Cyclic extensions of Moufang loops induced by semi-automorphisms*, J. Algebra Appl. **13**, (2014), 7 pages

[5] P. Jedlička, M. Kinyon, P. Vojtěchovský: *Structure of commutative automorphic loops*, Trans. of AMS 363 (2011), no. 1, 365–384

[6] P. Jedlička, M. Kinyon, P. Vojtěchovský: *Constructions of commutative automorphic loops*, Commun. in Alg., vol. 38 Issue 9 (2010), 3243–3267

[7] P. Jedlička, D. Simon: *On commutative A-loops of order pq*, J. Algebra Appl. **14**,3 (2014), 20 pages

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

[9] H. O. Pflugfelder: "Quasigroups and Loops: Introduction" (1990) Berlin: Heldermann

7 Odd order semidirect extensions of commutative automorphic loops

Přemysl Jedlička

Abstract

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

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

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

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

1 Preliminaries

We expect the reader to be already familiar with basic definitions in the loop theory. If not, we refer to [6]. Unlike most loop theory papers, we shall use the additive notation here rather than the multiplicative one; the reason is that subgroups of our loops will appear as aditive groups of rings.

In this section, we shall recall the semidirect construction presented in [2]. A semidirect product is a configurations of subloops in a loop $(Q,+)$: we have $H < Q$ and $K \triangleleft Q$ such that $K+H=Q$ and $K \cap H = 0$. In [2] an external point of view was given, assuming additionaly that $K \leqslant N_\mu(Q)$ and K being an abelian group. Such loops can be constructed given a special mapping φ.

Proposition 1.1 ([2]). *Let H and K be abelian groups and let us have a mapping $\varphi : H^2 \to \mathrm{Aut}(K)$. We define an operation $*$ on $Q = K \times H$ as follows:*

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

This loop is denoted by $K \rtimes_\varphi H$. Let us denote $\varphi_{i,j,k} = \varphi_{i,j+k} \circ \varphi_{j,k}$. Then Q is a commutative A-loop if and only if the following properties hold:

$$\varphi_{i,j} = \varphi_{j,i} \tag{1}$$
$$\varphi_{0,i} = \mathrm{id}_K \tag{2}$$
$$\varphi_{i,j} \circ \varphi_{k,n} = \varphi_{k,n} \circ \varphi_{i,j} \tag{3}$$
$$\varphi_{i,j,k} = \varphi_{j,k,i} = \varphi_{k,i,j} \tag{4}$$
$$\varphi_{i,j+k} + \varphi_{j,i+k} + \varphi_{k,i+j} = \mathrm{id}_K + 2 \cdot \varphi_{i,j,k} \tag{5}$$

Moreover, $K \times 0$ is a normal subgroup of Q, $0 \times H$ is a subgroup of Q and $(K \times 0) \cap (0 \times H) = 0 \times 0$ and $(K \times 0) + (0 \times H) = Q$.

Q is associative if and only if $\varphi_{i,j} = \mathrm{id}_K$, for all $i, j \in H$. The nuclei are $N_\mu(Q) = K \times \{i \in H;\ \forall j \in H : \varphi_{i,j} = \mathrm{id}_K\}$ and $N_\lambda = \{a \in K;\ \forall j, k \in H :\ \varphi_{j,k}(a) = a\} \times \{i \in H;\ \forall j \in H :\ \varphi_{i,j} = \mathrm{id}_K\}$.

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

Proposition 1.2. *Let $Q_1 = K \rtimes_\varphi H$ and $Q_2 = K \rtimes_\psi H$ be two semidirect products such that, for each $i \in H$, there exists $j \in H$ such that $\varphi_{ij} \neq \mathrm{id}_K$. Then $Q_1 \cong Q_2$ if and only if there exist $\alpha \in \mathrm{Aut}(K)$ and $\beta \in \mathrm{Aut}(H)$ such that $\alpha\varphi_{i,j} = \psi_{\beta(i),\beta(j)}\alpha$, for all $i, j \in H$.*

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

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

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

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

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

Now we compute

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

We finally compute

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

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

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

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

Proposition 1.3. *Let $K = K_1 \times K_2$ and suppose that φ splits on K, meaning that, there exist $\bar\varphi : H^2 \to \mathrm{Aut}(K_1)$ and $\bar{\bar\varphi} : H^2 \to \mathrm{Aut}(K_2)$ such that $\varphi_{i,j}((a_1,a_2)) = (\bar\varphi_{i,j}(a_1), \bar{\bar\varphi}_{i,j}(a_2))$, for each $i, j \in H$. Then $K \rtimes_\varphi H$ is the pullback of $K_1 \rtimes_{\bar\varphi} H$ and $K_2 \rtimes_{\bar{\bar\varphi}} H$. In particular, if $\bar\varphi$ is trivial then $K \rtimes_\varphi H \cong K_1 \times (K_2 \rtimes_{\bar{\bar\varphi}} H)$.*

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

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

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

The particular case is clear. □

2 Extension of order 3

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

Proposition 2.1. *Let $H = \mathbb{Z}_3$. Then ϕ satisfies Conditions* (1)–(5) *if and only if there exists an automorphism α of K such that $4\alpha^2 - 5\alpha + 1 = 0$, $\phi_{1,2} = \phi_{2,1} = \alpha$ and $\varphi_{1,1} = \varphi_{2,2} = 2\alpha - 1$.*

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

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

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

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

Lemma 2.2. *Let $Q_1 = K \rtimes_\varphi \mathbb{Z}_3$ and $Q_2 = K \rtimes_\psi \mathbb{Z}_3$ be two automorphic loops. Then $Q_1 \cong Q_2$ if and only if $\varphi_{1,2}$ and $\psi_{1,2}$ are conjugate in* $\mathrm{Aut}(K)$.

Proof. If $\varphi_{1,2} = \alpha\psi_{1,2}\alpha^{-1}$ then, according to Proposition 2.1, $\varphi_{i,j} = \alpha\psi_{j,i}\alpha^{-1}$, for any $i, j \in \mathbb{Z}_3$ and Q_1 and Q_2 are isomorphic due to Proposition 1.2.

On the other hand, if $\varphi_{1,2} = 1$ then φ is trivial, according to Proposition 2.1, and the resulting loop is a direct product. But this means that ψ is trivial too and $\varphi_{1,2} = \psi_{1,2}$.

Suppose hence $\varphi_{1,2} = \varphi_{2,1} \neq 1$. Proposition 2.1 states, that $\psi_{i,j} = \psi_{\beta(i),\beta(j)}$, for both the possible automorphisms β and any $i, j \in \mathbb{Z}_3$. Now, if $\alpha\varphi_{1,2} = \psi_{1,2}\alpha$ then $\alpha\varphi_{1,1} = \psi_{1,1}\alpha$ since $\varphi_{1,1}$ and $\psi_{1,1}$ are already determined. □

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

Proposition 2.3. *Let K be a vector space over a field F of dimension n. If* $\mathrm{char}(F) = 2$ *then every semidirect product $K \rtimes \mathbb{Z}_3$ yielding an automorphic loop is direct. If* $\mathrm{char}(F) = 3$ *then there exist, up to isomorphism, $\lceil \frac{n}{2} \rceil$ semidirect products $K \rtimes \mathbb{Z}_3$ that are automorphic loops. Otherwise, there are $n+1$ such loops, up to isomorphism.*

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

Let α now be a solution of the quadratic equation $4x^2 - 5x + 1 = 0$. The minimal polynomial of α divides $4x^2 - 5x + 1$ and therefore, if the characteristic differs from 3, α is similar to a diagonal matrix with entries in $\{1, \frac{1}{4}\}$. There are $n + 1$ such matrices, up to similarity, which is, according to Lemma 2.2, the only criterion for an isomorphism.

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

It is useful to note that, in the previous case, the fundamental loop construction is the semidirect product $K \rtimes_\varphi \mathbb{Z}_3$ with $\dim K = 2$ and $\varphi_{1,2} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ in characteristic 3 and $\dim K = 1$ and $\varphi_{1,2} = \frac{1}{4}$ in different characteristic. The other constructions can be obtained using pullbacks and direct products as stated in Proposition 1.3.

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

Lemma 2.4 (Hensel)**.** *Let f be a polynomial in $\mathbb{Z}[x]$ let p be a prime, let $m, k \in \mathbb{N}$ and let $r \in \mathbb{Z}$ such that*

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

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

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

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

Proposition 2.5. *Let $K = \mathbb{Z}_{p^k}$, for some odd prime k. Then there exist two non-isomorphic automorphic loops $\mathbb{Z}_{p^k} \rtimes_\varphi \mathbb{Z}_3$ for $p > 3$, one for $p^k = 3$, three for $p^k = 9$ and six such loops if $p = 3$ and $k > 2$.*

Proof. Every automorphism is equivalent to multiplication by an invertible element and all the automorphisms commute. Hence distinct automorphisms never conjugate and different constructions give rise to different loops, according to Lemma 2.2. If $p > 5$ then the polynomial $4x^2 - 5x + 1$ from Proposition 2.1 has two distinct roots, according to Hensel's lemma.

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

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

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

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

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

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

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

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

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

It was already observed in Proposition 1.3 that the decomposition of K gives the decomposition of $K \rtimes_\varphi H$ as a pullback. This means that the only case left to count the number of different $K \rtimes_\varphi \mathbb{Z}_3$, for an arbitrary finite K, is the case $K \cong \prod \mathbb{Z}_{p^{e_i}}$. However this would need the description of conjugacy classes of isomorphisms in such groups and this is out of the scope of this article.

3 Extension of 2-divisible groups

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

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

Lemma 3.1. *Let φ satisfy* (1)–(5). *Then*

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

for any $i, j \in H$.

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

Lemma 3.1 states that, for a uniquely 2-divisible group K, any $\varphi_{i,j}$ can be expressed in terms of mappings $\varphi_{k,-k}$; for the sake of brevity, we shall write φ_k as an abbreviation for $\varphi_{k,-k}$. Note that $\varphi_i = \varphi_{-i}$.

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

Lemma 3.2. *Let $i, j, k \in H$ and let φ satisfy* (1)–(5)*. Then*

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

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

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

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

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

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

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

□

Theorem 3.3. *Let K and H be uniquely 2-divisible abelian groups and let $\varphi : H^2 \to \mathrm{Aut}(K)$. Then φ satisfies*

condition (1) *to* (5) *if and only if*

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

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

$$\varphi_0 = 1, \tag{9}$$

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

Proof. The necessity of the conditions was already proved in Lemmas 3.1 and 3.2 and hence we prove the sufficiency only. Conditions (1) and (2) follow immediately from (6) and (9). Condition (7) shows that the subring generated by all the φ_i, $i \in H$ is commutative, thus giving (3). In Lemma 3.2 we proved (1), (2), (3), (6), (7) $\Rightarrow$ (8) and we clearly see (8) $\Rightarrow$ (4). The only remaining condition is thus (5).

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

4 Extension of order 5

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

Proposition 4.1. *Let* $Q = K \rtimes_\varphi \mathbb{Z}_5$ *be a semidirect product. Then* Q *is automorphic if and only if there exists* $\alpha \in \mathrm{Aut}\, K$ *such that* $\varphi_1 = \varphi_4 = \alpha$, $\varphi_2 = \varphi_3 = 4\alpha^2 - 4\alpha + 1$ *and* $16\alpha^3 - 28\alpha + 13\alpha - 1 = 0$.

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

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

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

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

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

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

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

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

Proposition 4.2. *Let* $K = \mathbb{Z}_p$, *for some odd prime* p. *Then there exist two non-isomorphic automorphic loops* $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_5$ *if and only if* 5 *is a quadratic residue in* $\mathbb{Z}_p$. *Otherwise there exists only one.*

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

Suppose now that 5 is a quadratic residue. There are 3 possible choices of φ, according to Proposition 4.1, namely

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

The latter two choices give isomorphic loops due to Proposition 1.2; we can set $\alpha = 1$ and $\beta = 2$. Hence we have two isomorphism classes, one associative and one non-associative. □

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

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

References

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

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

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

[4] P. Jedlička, M. Kinyon, P. Vojtěchovský: *Constructions of commutative automorphic loops*, Commun. in Alg., vol. 38 Issue 9 (2010), 3243–3267

[5] P. Jedlička, D. Simon: *On commutative A-loops of order pq*, J. Algebra Appl. **14**,3 (2014), 20 pages

[6] H. O. Pflugfelder: "Quasigroups and Loops: Introduction" (1990) Berlin: Heldermann