Commutative automorphic p-loops

Přemysl Jedlička[⋆]
e-mail: jedlickap@tf.czu.cz
Czech University of Life Sciences, Czech Republic
Michael Kinyon
e-mail: mkinyon@math.du.edu
Denver University, USA
Petr Vojtěchovský
e-mail: petr@math.du.edu
Denver University, USA

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* $\mathrm{Mlt}(Q) = \langle L_x, R_x |\ x \in Q \rangle$. The inner mapping group $\mathrm{Inn}(Q) = \mathrm{Mlt}(Q)_1$ is the stabilizer of $1 \in Q$.

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 [1]. The study of A-loops was initiated by Bruck and Paige [2]. They obtained many basic results for A-loops, not the least of which is that A-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.

The bulk of [2] 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 [9] in the commutative case, and Kinyon, Kunen and Phillips [8] in the general case. Moufang A-loops have been used to characterize a certain class of quasigroups [7], and have been shown to have an affirmative answer for the restricted Burnside problem [10].

For *commutative* automorphic loops, there now exists a detailed structure theory [4], as well as constructions and small order classification results [5]. For each prime p, a commutative A-loop has order a power of p if and only i f every element has order a power of p. We may thus refer to such loops unambiguously as commutative automorphic *p-loops*.

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 by

$$Z(Q) = \{a \in Q \mid L_a = R_a \in Z(\mathrm{Mlt}(Q))\}.$$

The center is a normal subloop of 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, and if for some n, $Z_{n-1}(Q) < Z_n(Q) = Q$, then Q is said to be *(centrally) nilpotent of class n*.

A classic result of group theory is that p-groups are nilpotent. This does not hold for loops in general, although it does hold in certain varieties of loops, such as Moufang loops [1]. It is not true, for instance, for commutative automorphic 2-loops. Indeed, there exist commutative A-loops of exponent 2 with trivial center [5]. The construction is the following:

Proposition 1. *Let $(G, \cdot)$ be an elementary abelian 2-group and let $Q = G \dot\cup \bar{G}$. Let f be an automorphism of G. We define an operation $*$ on Q as follows:*

$$a * b = a \cdot b \qquad a * \bar{b} = \bar{a} * b = \overline{a \cdot b} \qquad \bar{a} * \bar{b} = f(a \cdot b).$$

Then $(Q, *)$ is a comutative automorphic 2-loop. If f is identity then Q is a group, otherwise $Z(Q) = \{a \in G \mid f(a) = a\}$.

The odd order is different. As noted in [4], every finite, power-associative commutative loop is uniquely 2-divisible if and only if it has odd order. A loop is *uniquely 2-divisible* if the squaring map $x \mapsto x^2$ is a permutation. We can associate, to every uniquely 2-divisible commutative A-loop, a *Bruck loop* of the same order and this loop bears some of the original loop's properties. This fact was used to establish *Lagrange*, *Hall*, *Sylow* and *Cauchy* theorems for commutative A-loops of odd order.

In [4], the following problem naturally appeared: does there exist an odd prime p and a commutative automorphic p-loop with trivial center? The main result of [6] gives a negative answer to this question.

Theorem 2. *Let p be an odd prime and let Q be a commutative automorphic p-loop. Then Q is centrally nilpotent.*

This theorem is in some sense the best possible result for automorphic p-loops. In particular, for each odd prime p, there exists a noncommutative automorphic loop of order p^3 and exponent p with trivial center.

Once we know that every commutative automorphic p-loop has a non-trivial center, we can possibly construct every such a loop using central extensions. It is not difficult to prove that every commutative A-loop of order p or p^2 has to be a group. For loops of order p^3, the central extensions can be based on overflows in modular arithmetic, as was shown in [5].

Proposition 3. *For $n \geq 1$ and $a, b \in Z_n$, define $\mathcal{Q}_{a,b}(\mathbb{Z}_n)$ on $\mathbb{Z}_n^3$ by*

$$\begin{aligned}(x1, x2, x3)(y1, y2, y3) = \\ (x1 + y1 + (x2 + y2)x3y3 + a(x2, y2)_n + b(x3, y3)_n,\ x2 + y2,\ x3 + y3),\end{aligned}$$

where the function $(-;-)_n : \mathbb{Z}_n^2 \to \{0, 1\}$ is the overflow generator *defined by*

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

Then Q is a commutative A-loop with $Z(Q) = \mathbb{Z}_n \times 0 \times 0$.

It is conjectured that different choices of a and b give raise to four non-isomorphic loops of order p^3 and that the construction is complete, i.e. there exist no more than these four commutative automorphic loops of order p^3, up to isomorphism.

References

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

[2] R. H. Bruck and 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** (2008), 357–382.

[4] P. Jedlička, M. K. Kinyon and P. Vojtěchovský, *The structure of commutative automorphic loops*, to appear in Proceedings of AMS

[5] P. Jedlička, M. K. Kinyon and P. Vojtěchovský, *Constructions of commutative automorphic loops*, to appear in Commun. in Alg.

[6] P. Jedlička, M. K. Kinyon and P. Vojtěchovský, *Commutative automorphic loops of odd prime power order*, preprint

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

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

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

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