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
   DOI: 10.1080/00927870903200877

3. Přemysl Jedlička, Michael K. Kinyon, Petr Vojtěchovský:
   The structure of commutative automorphic loops,
   Transactions of American Mathematical Society **363**,1 (2011), 365–384
   DOI: 10.1090/S0002-9947-2010-05088-3

4. Přemysl Jedlička, Michael K. Kinyon, Petr Vojtěchovský:
   Nilpotency in automorphic loops of prime power order,
   Journal of Algebra **350** (2012), 64–76
   DOI: 10.1016/j.jalgebra.2011.09.034

5. Přemysl Jedlička, Denis Simon:
   On commutative A-loops of order pq,
   Journal of Algebra and its Applications **14**,3 (2014), 20 pages
   DOI: 10.1142/S0219498815500413

6. Jan Hora, Přemysl Jedlička:
   Nuclear semidirect product of commutative automorphic loops,
   Journal of Algebra and its Applications **13**,1 (2014), 15 pages
   DOI: 10.1142/S0219498813500771

7. Přemysl Jedlička:
   Odd order semidirect extensions of commutative automorphic loops,
   Commentationes Mathematicae Universitatis Carolinae **55**,4 (2014), 447–456
   `https://cmuc.karlin.mff.cuni.cz/pdf/cmuc1404/jedlic.pdf`

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:

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

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