

Finite commutative automorphic loops

Gábor Péter Nagy

University of Szeged (Hungary)

3rd Mile High Conference, Denver, August 11-17, 2013

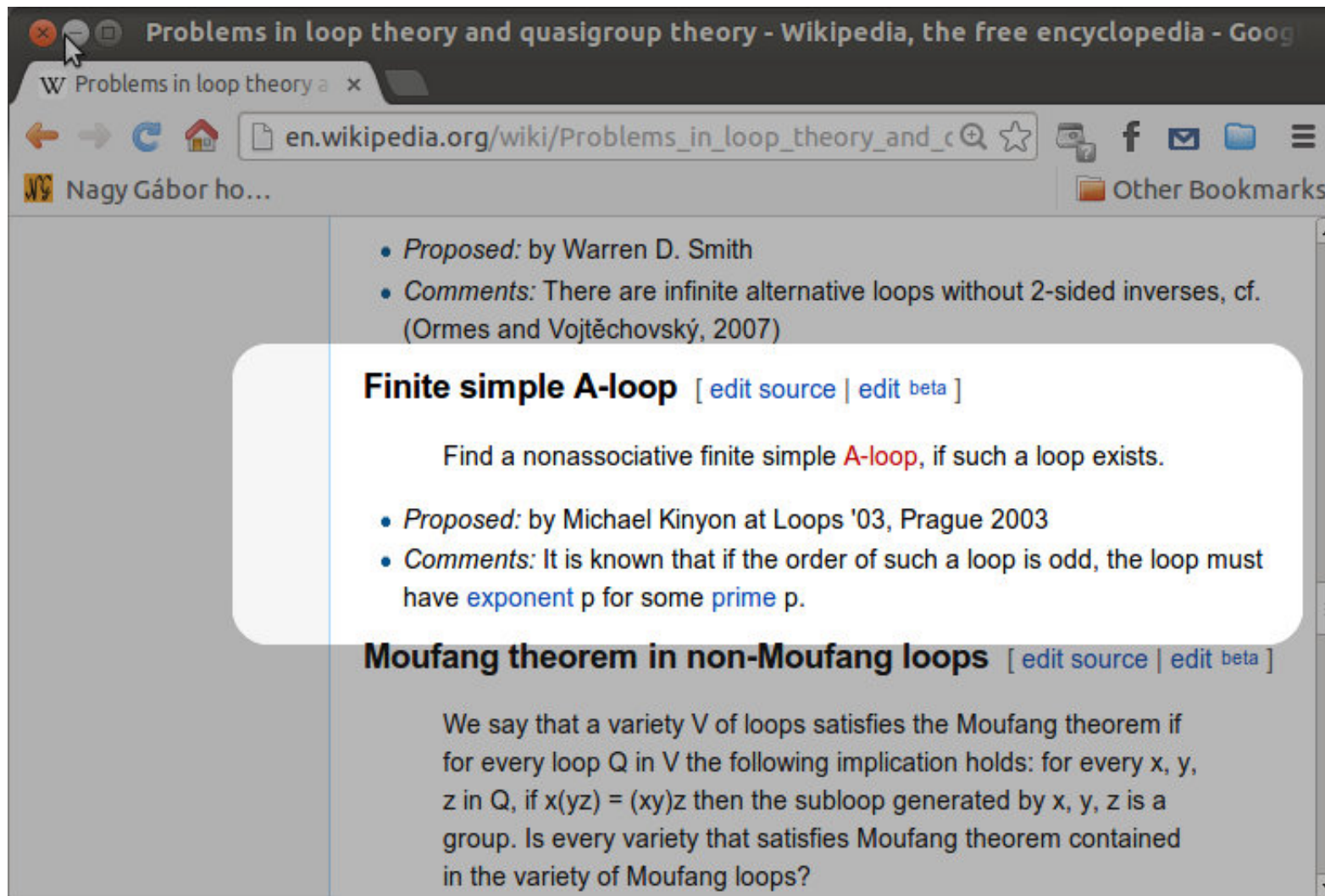
Overview

- 1 Automorphic loops
- 2 Finite simple commutative A-loops
- 3 Centerless finite commutative A-loops of exponent 2

Basic concepts

- Left and right multiplication maps: L_x, R_x
- Multiplication group, inner mapping group: $\text{Mlt}(Q), \text{Inn}(Q)$
- Normal subloop, center, factor loop
- Solvable loop, simple loop
- Automorphic loop (A-loop): $\text{Inn}(Q) \leq \text{Aut}(Q)$
- Power-associativity, p -loop
- Anti-automorphic inverse property: $(xy)^{-1} = y^{-1}x^{-1}$

Problem setting



The screenshot shows a web browser window with the title "Problems in loop theory and quasigroup theory - Wikipedia, the free encyclopedia - Google". The address bar shows the URL "en.wikipedia.org/wiki/Problems_in_loop_theory_and_c". The page content includes a list of problems:

- *Proposed:* by Warren D. Smith
- *Comments:* There are infinite alternative loops without 2-sided inverses, cf. (Ormes and Vojtěchovský, 2007)

Finite simple A-loop [[edit source](#) | [edit beta](#)]

Find a nonassociative finite simple **A-loop**, if such a loop exists.

- *Proposed:* by Michael Kinyon at Loops '03, Prague 2003
- *Comments:* It is known that if the order of such a loop is odd, the loop must have **exponent** p for some **prime** p .

Moufang theorem in non-Moufang loops [[edit source](#) | [edit beta](#)]

We say that a variety V of loops satisfies the Moufang theorem if for every loop Q in V the following implication holds: for every x, y, z in Q , if $x(yz) = (xy)z$ then the subloop generated by x, y, z is a group. Is every variety that satisfies Moufang theorem contained in the variety of Moufang loops?

Previous work done by



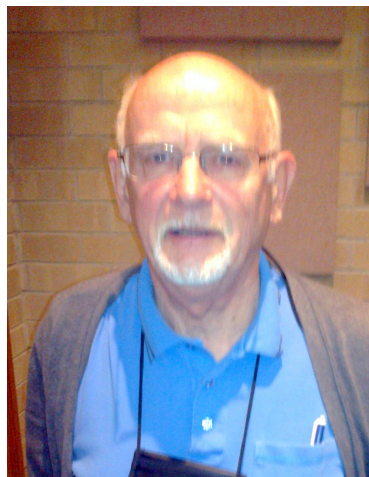
Přemysl



Michael



Petr



Ken



J. D.



Piroska

Previous results

Theorem (Albert 1943)

Q is simple if and only if $\text{Mlt}(Q)$ acts primitively on Q .

Proposition

Let Q be a finite, commutative automorphic loop.

- 1 $Q \cong O(Q) \times E(Q)$ where $|O(Q)|$ is odd and $E(Q)$ is a 2-loop.
- 2 If $|Q|$ is odd, then Q is solvable.
- 3 If Q is simple, then Q has exponent 2.

Proposition

Every A-loop has the anti-automorphic inverse property:

$$JL_xJ = R_x^{-1}.$$

Main result

Main theorem (Grishkov, Kinyon, N 2012)

- 1 Every finite, commutative automorphic loop is solvable.
- 2 Every automorphic 2-loop is solvable.

Main strategies:

- Heavy **equational computations**, by hand and Prover9.
- Deep results from the theory of **finite groups**.
- Deep results from the theory of **Lie rings**.

Proposition

Every finite simple, automorphic 2-loop is **commutative** of exponent 2.

Commutative A-loops of exponent 2 and Lie rings

- Let (Q, \circ) be a **finite simple commutative A-loop of exponent 2**.
- Using **deep group theory**, we show that $\text{Mlt}(Q)$ is a primitive group of **affine type**.
- This defines an **elementary abelian 2-group** operation $(Q, +)$.
- Define the bracket $[x, y] = x + y + x \circ y$.
- **(Wright 1969)** $(Q, +, [\cdot, \cdot])$ is a **simple nonassociative algebra** over \mathbb{F}_2 .

Proposition

$(Q, +, [\cdot, \cdot])$ is a **simple Lie algebra** over \mathbb{F}_2 satisfying

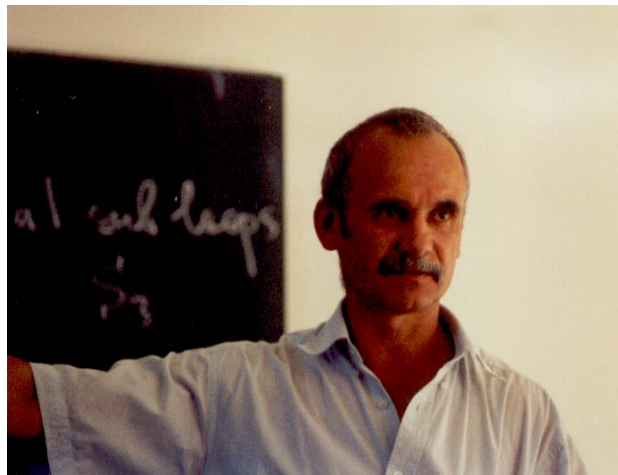
$$\text{ad}(u) \text{ad}([u, w]) = 0$$

for all $u, w \in Q$.

The “crust of a thin sandwich”



Efim Zel'manov



Grishkov at LOOPS'03

Theorem (Zel'manov, Kostrikin 1990)

Let \mathfrak{g} be a Lie ring generated by a finite collection of elements a satisfying $\text{ad}(a)^2 = 0$ and $\text{ad}(a)\text{ad}(x)\text{ad}(a) = 0$ for all $x \in \mathfrak{g}$. Then \mathfrak{g} is nilpotent.

Proof of the Main Theorem. Some more juggling with equations shows that ZK applies for $(Q, +, [\cdot, \cdot])$, a contradiction. \square

Automorphic p -loops and nilpotency

Previous results (Jedlička, Kinyon, Vojtěchovský, Csörgő 2010/11)

- 1 For $p > 2$, commutative automorphic p -loops are **nilpotent**.
- 2 There are nonnilpotent automorphic p -loops **for $p > 2$** .
- 3 There are nonnilpotent **commutative** automorphic 2-loops.

The construction

Theorem 1

Let n, m be positive integers, $\beta : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^{n \times n}$ a linear map such that $y, y' \in \mathbb{F}_2^m$

- ① $I + \beta(y)$ is nonsingular, and
- ② $\beta(y), \beta(y')$ commute.

Define the operation \circ on \mathbb{F}_2^{n+m} by

$$(x_1, y_1) \circ (x_2, y_2) = (x_1 + x_2 + \beta(y_1)x_2 + \beta(y_2)x_1, y_1 + y_2). \quad (1)$$

Then $(\mathbb{F}_2^{n+m}, \circ, 0)$ is a commutative A-loop of exponent 2.

Note that with

$$[(x_1, y_1), (x_2, y_2)] = [\beta(y_1)x_2 + \beta(y_2)x_1, 0],$$

$(\mathbb{F}_2^{n+m}, +, [\cdot, \cdot])$ is a solvable Lie algebra of characteristic 2.

Centerless commutative A-loops of exponent 2

Theorem 2

$(\mathbb{F}_2^{n+m}, \circ)$ has trivial center if and only if $\beta(y)$ is nonsingular for all $y \in \mathbb{F}_2^m$. In particular, in the centerless case $m < n$.

Example

Let $m < n$, $m \mid n$ and fix $\alpha \in \mathbb{F}_2^n \setminus \mathbb{F}_2^m$. Define β by

$$\beta(y)x = \alpha xy.$$

Then the corresponding comm. A-loop of exp. 2 has trivial center.

Remarks.

- ① Additively closed subsets of $GL(n, p) \cup \{0\}$ are interesting on their own. [\rightsquigarrow partial additive spreads]
- ② **PROBLEM:** \exists infinite simple comm. A-loops of exp. 2 ???

The End

THANK YOU FOR YOUR ATTENTION!