Totally Automorphic Loops

Michael Kinyon

Department of Mathematics

University of Denver

3rd Mile High Conference on Nonassociative Mathematics,
University of Denver, Denver, CO, USA
12 August 2013

Loops

Definition (Combinatorial)

A *quasigroup* $(Q, \cdot)$ is a set Q with a binary operation $\cdot$ such that for each $a, b \in Q$, the equations $ax = b$ and $ya = b$ have unique solutions $x, y \in Q$.

Definition (Universal algebra)

A *quasigroup* $(Q, \cdot, \backslash, /)$ is a set Q with three binary operations satisfying $x\backslash(xy) = y = x(x\backslash y)$ and $(xy)/y = x = (x/y)y$.

A *loop* is a quasigroup with an identity element.

Multiplication tables of loops $=$ normalized Latin squares

Multiplications and Divisions

In a loop Q, the *left* and *right multiplication maps*

$$L_x : Q \to Q; \quad L_x y = xy$$
$$R_x : Q \to Q; \quad R_x y = yx$$

are permutations. So are the *division maps*

$$M_x : Q \to Q; \quad M_x y = y \backslash x$$
$$M_x^{-1} : Q \to Q; \quad M_x^{-1} y = x/y\,.$$

Permutation Groups

Various permutation groups act on loops:

$\mathrm{Mlt}(Q) = \langle L_x, R_x \mid x \in Q \rangle$	*multiplication group*
$\mathrm{Inn}(Q) = \mathrm{Stab}_{\mathrm{Mlt}(Q)}(1)$	*inner mapping group*
$\mathrm{TMlt}(Q) = \langle L_x, R_x, M_x \mid x \in Q \rangle$	*total multiplication group*
$\mathrm{TInn}(Q) = \mathrm{Stab}_{\mathrm{TMlt}(Q)}(1)$	*total inner mapping group*
$\mathrm{Aut}(Q)$	*automorphism group*

The total multiplication and total inner mapping groups are not as familiar as the others. Their importance to loop theory has been highlighted recently by Stanovský and Vojtěchovsky. (They will speak about this and other things on Friday.)

Generators of $\mathrm{Inn}(Q)$

For any loop Q, $\mathrm{Inn}(Q)$ has a set of convenient generators:

$$\begin{aligned} T_x &= L_x^{-1} R_x && \text{(generalized conjugations)} \\ L_{x,y} &= L_{xy}^{-1} L_x L_y && \text{(measures of} \\ R_{x,y} &= R_{yx}^{-1} R_x R_y && \text{nonassociativity)} \end{aligned}$$

$\mathrm{TInn}(Q)$ also has various sets of generators, none of which are as “nice” as those for $\mathrm{Inn}(Q)$.
A nice special case is inverse property loops. In such a loop, $\mathrm{TInn}(Q) = \langle \mathrm{Inn}(Q), J \rangle$ where $Jx = x^{-1}$.

Automorphic Loops

Definition

A loop Q is said to be *automorphic* if $\mathrm{Inn}(Q) \leq \mathrm{Aut}(Q)$.

Examples:

- Groups
- Commutative Moufang loops (but not all Moufang loops)
- More in the talks of Nagý and Jedlička (today) and Aboras (Friday)

UA perspective

The condition of being automorphic can be expressed as three universally quantified equations by using the generators of $\mathrm{Inn}(Q)$.
Thus automorphic loops form a *variety* (in the universal algebra sense) and so ...

- Homomorphic images,
- Subloops, and
- Products

of automorphic loops are automorphic.

History

Automorphic loops (under the name “A-loops”) were introduced by Bruck and Paige in

Loops whose inner mappings are automorphisms,
Ann. of Math. (2) **63** (1956), 308–323.

History

Automorphic loops (under the name “A-loops”) were introduced by Bruck and Paige in

Loops whose inner mappings are automorphisms,
Ann. of Math. (2) **63** (1956), 308–323.

- Bruck’s interest: Commutative Moufang loops are A-loops. How much of their structure comes from that fact?

History

Automorphic loops (under the name “A-loops”) were introduced by Bruck and Paige in

Loops whose inner mappings are automorphisms, *Ann. of Math.* (2) **63** (1956), 308–323.

- Bruck’s interest: Commutative Moufang loops are A-loops. How much of their structure comes from that fact?
- Paige’s interest: he was Bruck’s student.

Basic properties

Theorem

Automorphic loops...

- *are flexible:* $xy \cdot x = x \cdot yx$ *[B&P 1956]*
- *are power-associative:* $x^m \cdot x^n = x^{m+n}$ *[B&P 1956]*
- *have the antiautomorphic inverse property*

$$(xy)^{-1} = y^{-1}x^{-1}$$

[Johnson, MK, Nagý & PV 2011]

Diassociative, automorphic loops

A loop is *diassociative* if any 2-generated subloop is associative. Informally, this just means that any expression involving at most two variables associates, such as $(xx)y = x(xy)$, $(xy)x = x(yx)$ and so on.

Diassociative, automorphic loops

A loop is *diassociative* if any 2-generated subloop is associative. Informally, this just means that any expression involving at most two variables associates, such as $(xx)y = x(xy)$, $(xy)x = x(yx)$ and so on.

1956 Bruck & Paige (implicitly) conjectured that every diassociative automorphic loop is a Moufang loop.

1958 Osborn: affirmative in the *commutative* case.

2000 K., Kunen & Phillips: affirmative in general.

The Commutative Case

Combining various papers, we have:

Theorem

Let Q be a finite commutative automorphic loop. Then

1. $Q \cong H \times K$ *where H is a 2-loop and K has odd order;*
2. *(Lagrange) The order of any subloop of Q divides $|Q|$;*
3. *Q is solvable;*
4. *(Sylow/Hall) For any set π of primes, Hall π-subloops exist.*

Parts (1) and (2) are from [Jedlička, MK, PV 2011].
Part (3) will be discussed by Nagý in the next talk.
Part (4) is from [Greer 2013].

General Case

Theorem (KKPV 2013)

Every automorphic loop of odd order is solvable.

In my opinion, this is the main open problem of (finite) loop theory:

Problem

Does there exist a finite simple nonassociative automorphic loop?

By exhaustive search, there is no such loop of order < 2500 (Johnson, MK, Nagý, PV 2011).

Definition

Call a loop Q *totally automorphic* if

$$\mathrm{TInn}(Q) \leq \mathrm{Aut}(Q)\,.$$

Definition

Call a loop Q *totally automorphic* if

$$\mathrm{TInn}(Q) \leq \mathrm{Aut}(Q)\,.$$

(As we will see shortly, this terminology is unnecessary.)

Definition

Call a loop Q *totally automorphic* if

$$\mathrm{TInn}(Q) \leq \mathrm{Aut}(Q)\,.$$

(As we will see shortly, this terminology is unnecessary.)

Inversion $M_1(x) = x\backslash 1 = x^{-1}$ is totally inner, so we have $(xy)^{-1} = x^{-1}y^{-1}$, the automorphic inverse property. But we also have the antiautomorphic inverse property, so…

Lemma

Totally automorphic loops are commutative.

The Punchline

Theorem

For a loop Q, the following are equivalent:

1. *Q is totally automorphic.*
2. *Q is*

The Punchline

Theorem

For a loop Q, the following are equivalent:

1. *Q is totally automorphic.*
2. *Q is a commutative Moufang loop.*

This turns out be a corollary of a *new* result. . . .

Result of 11 August!

More generally...

Theorem

For a loop Q, the following are equivalent:

1. $\langle\, L_{x\backslash y}^{-1} M_y M_x,\, R_{y/x}^{-1} M_y^{-1} M_x^{-1} \mid x, y \in Q \,\rangle \leq \mathrm{Aut}(Q).$
2. *Q is an automorphic Moufang loop.*

Idea of Proof: (2)⇒(1) is easy. For (1)⇒(2),

- By a slightly messy automated proof, Q has the inverse property.
- In inverse property loops, the group above is $\mathrm{Inn}(Q)$, so Q is automorphic.
- Hence by Bruck & Paige, Q is diassociative.
- Hence by MK, Kunen & Phillips, Q is Moufang.

Question

What other interesting varieties of loops can be characterized by specifying that some group of total inner mappings acts as automorphisms?