Automorphic loops and their associated permutation groups

Michael K. Kinyon

Department of Mathematics

University of Denver

LMS Symposium, Durham, UK, 21 July 2015

Combinatorial definition

A *loop* $(Q, \cdot)$ is a set Q with a binary operation $\cdot$ such that
(1) there is an identity element $1 \cdot x = x \cdot 1 = x$.
(2) for each $a, b \in Q$, the equations

$$ax = b \qquad \text{and} \qquad ya = b$$

have unique solutions $x, y \in Q$.

Combinatorial definition

A *loop* $(Q,\cdot)$ is a set Q with a binary operation $\cdot$ such that
(1) there is an identity element $1\cdot x = x\cdot 1 = x$.
(2) for each $a, b \in Q$, the equations

$$ax = b \qquad \text{and} \qquad ya = b$$

have unique solutions $x, y \in Q$.

Multiplication tables of loops = reduced Latin squares

Example:

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

Universal algebra definition

A *loop* $(Q, \cdot, \backslash, /, 1)$ is a set Q with an identity element $1x = x1 = x$ and three binary operations $\cdot$, $\backslash$, $/$ such that for all $x, y \in Q$:

$$x\backslash(xy) = y \qquad x(x\backslash y) = y$$
$$(xy)/y = x \qquad (x/y)y = x$$

This definition has advantages if the class of loops in which one is interested can be viewed as a variety.

Inner Mappings

In a loop Q, the *left* and *right translations*

$$L_x : Q \to Q; \quad yL_x = xy \qquad R_x : Q \to Q; \quad yR_x = yx$$

are permutations.

Various permutation groups act on loops:

- The *multiplication group* $\mathit{Mlt}\, Q = \langle L_x, R_x | x \in Q\rangle$
- The *inner mapping group* $\mathit{Inn}\, Q = (\mathit{Mlt}\, Q)_1$ (stabilizer of $1 \in Q$)
- The *automorphism group* $\mathit{Aut}\, Q$

Generators

For any loop Q, $Inn(Q)$ has a set of canonical generators:

$$T_x = R_x L_x^{-1} \qquad \text{(generalized conjugations)}$$

$$L_{x,y} = L_x L_y L_{yx}^{-1} \qquad \text{(measures of}$$

$$R_{x,y} = R_x R_y R_{xy}^{-1} \qquad \text{nonassociativity)}$$

Thus conditions on $Inn(Q)$ can sometimes be expressed equationally.

Normality

Any of the following equivalent conditions can be used to define what it means for a subloop A of a loop Q to be *normal*:

- A is a block of $Mlt(Q)$ containing 1;
- A is $Inn(Q)$-invariant;
- $xA = Ax$, $x \cdot yA = xy \cdot A$, $Ax \cdot y = A \cdot xy$ for all $x, y \in Q$.

Solvability and simplicity

Solvability of a loop Q is defined just as for groups: there is an subnormal series $1 = H_0 < H_1 < \cdots < H_n = Q$ such that each factor H_{j+1}/H_j is an abelian group.

A loop is *simple* if it has no nontrivial normal subloops.

Using the multiplication group

Theorem (Albert '41)

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

Theorem (Vesanen '94)

If Q is finite and $\mathrm{Mlt}(Q)$ is solvable, then Q is solvable.

Thus the multiplication groups of finite simple loops are nonsolvable and primitive.

Bruck and Paige

Definition

A loop is *automorphic* (or an *A-loop*, for short) if $\mathit{Inn}\, Q \leq \mathit{Aut}\, Q$.

These were introduced by Bruck and Paige in 1956 in the last loop theory paper which ever appeared in *Annals*.

Bruck and Paige provided very few examples, so let's jump out of historical order to give some.

Example

One of these is the smallest nonassociative automorphic loop ([KKPV] 2015). The other is $S_3 \cong D_3$. Can you tell which is which?

$\cdot$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	0	4	5	3
2	2	0	1	5	3	4
3	3	5	4	0	1	2
4	4	3	5	2	0	1
5	5	4	3	1	2	0

$\cdot$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	0	4	5	3
2	2	0	1	5	3	4
3	3	5	4	0	2	1
4	4	3	5	1	0	2
5	5	4	3	2	1	0

Dihedral automorphic loops

The preceding is a case of a general construction ([KKPV ’15], [Aboras ’14]).

Let $(A, +)$ be an abelian group, fix $\alpha \in Aut(A)$. On $\mathbb{Z}_2 \times A$, define

$$(i, u) \cdot (j, v) = (i + j, ((-1)^j u + v)\alpha^{ij}) .$$

This is a *dihedral automorphic loop*, which is a (generalized) dihedral group if $\alpha = 1$.

Lie algebra construction

(From [JKV '11])

Let $\mathbb{F}$ be a field and let $A \in GL(2, \mathbb{F})$ be such that $I + cA \in GL(2, \mathbb{F})$ for all $c \in \mathbb{F}$. On $\mathbb{F} \times \mathbb{F}^2$, define

$$(a, x) \cdot (b, y) = (a + b, x(I + bA) + y(I - aA)) .$$

This is an automorphic loop.

If $\mathbb{F} = \mathbb{R}$, this is a Lie loop of dimension 3.

If $\mathbb{F} = GF(p)$, this is a loop of order p^3 with trivial center!

Variety

The automorphic condition $Inn\,Q \leq Aut\,Q$ can be expressed as three universally quantified identities by using the standard generators of $Inn(Q)$:

$$\begin{aligned} xL_{z,u} \cdot yL_{z,u} &= (xy)L_{z,u} \\ xR_{z,u} \cdot yR_{z,u} &= (xy)R_{z,u} \\ xT_z \cdot yT_z &= (xy)T_z\,. \end{aligned}$$

Thus automorphic loops form a *variety* of loops, closed under taking subloops, direct products and homomorphic images.

Basic Facts

Basic facts about automorphic loops [BP ’56, JKNV ’10]

- $\langle L_x, R_x \mid x \in Q\rangle$ is an abelian group.
- Q is *power-associative*: each $\langle x\rangle$ is a group.
- Q has the *antiautomorphic inverse property*: $(xy)^{-1} = y^{-1}x^{-1}$.

Moufang loops

Moufang loops are probably more familiar to mathematicians than automorphic loops. Examples include the nonzero octonions, S^7 and the Parker loop used to construct the Monster.
"Most" Moufang loops are not automorphic. *Commutative* Moufang loops are. The smallest nonassociative automorphic Moufang loops (commutative or not) have order 81.

- Bruck's interest in A-loops: How much of the structure of commutative Moufang loops comes from their being A-loops?
- Paige's interest: he was Bruck's student.

B & P's Main Question

A loop is *diassociative* if every 2-generated subloop is associative.

Every Moufang loop is diassociative. (This is a corollary of Moufang's Theorem.)

B & P's Question: *Is every diassociative automorphic loop Moufang?*

Answers

- Yes, for commutative automorphic loops. (Osborn ’58)
- Yes, in general. (K, Kunen, Phillips 2002)

There were *no* papers on A-loops between those two, and none afterward for another 8 years.

Many knew what these loops were, but no one knew how to handle them.

Products of squares in commutative A-loops

A breakthrough came in 2009 for *commutative* automorphic loops.

In abelian groups (and commutative Moufang loops), the product of squares is (trivially!) a square:

$$x^2 y^2 = (xy)^2$$

Products of squares in commutative A-loops

A breakthrough came in 2009 for *commutative* automorphic loops.

In abelian groups (and commutative Moufang loops), the product of squares is (trivially!) a square:

$$x^2y^2 = (xy)^2$$

This is *false* in commutative A-loops. (The smallest counterexample has order 15.)

Products of squares in commutative A-loops

A breakthrough came in 2009 for *commutative* automorphic loops.

In abelian groups (and commutative Moufang loops), the product of squares is (trivially!) a square:

$$x^2 y^2 = (xy)^2$$

This is *false* in commutative A-loops. (The smallest counterexample has order 15.)

However, it *is* still true that the product of squares is a square:

Theorem

In a commutative A-loop,

$$x^2 y^2 = (yL_{y,x} \cdot xL_{x,y})^2$$

Commutative automorphic loops

Combining work of K, Jedlička, Vojtěchovský, Grishkov, Nagy, Greer. . . , we now know a lot!

Let Q be a commutative automorphic loop. Then. . .

- Q is solvable.
- $Q \cong O \times E$ where O has odd order and $|E|$ is power of 2.
- The Lagrange property holds.
- The Sylow & Hall (Existence) Theorems hold.
- If $|Q| = p^n$, $p > 2$, then Q is nilpotent.

The Main Problem

Problem

Do there exist finite simple nonassociative automorphic loops?

The Main Problem

Problem

Do there exist finite simple nonassociative automorphic loops?

Conjecture

No.

The Main Problem

Problem

Do there exist finite simple nonassociative automorphic loops?

Conjecture

No. More precisely...

Every finite simple automorphic loop is associative.

Odd Order Theorem

Theorem (K, Kunen, Phillips, Vojtěchovský (proved in 2011; to appear in 2015))

Every automorphic loop of odd order is solvable.

The easy part of the proof use some deep ideas of Glauberman to prove that a minimal counterexample Q must have exponent p. The hard part constructs a Lie algebra over $GF(p)$ on Q which is simultaneously simple and solvable to get a contradiction.

p-loops

Theorem (KKPV '15, GKN '14)

A finite automorphic p-loop is solvable.

The case p odd is covered by the Odd Order Theorem. The case $p = 2$ first reduces the problem to *exponent* 2. Then we construct a Lie algebra over $GF(2)$ on the same set which is both simple and nilpotent. This uses the Kostrikin-Zelmanov "Crust of a Thin Sandwich" theorem.

Socle

Theorem (KKPV '15)

If Q is finite simple nonassociative automorphic loop, then $\mathrm{Soc}(Mlt(Q))$ is not regular.

So if we attack the problem via O'Nan-Scott, this eliminates affine and twisted affine types.

2-Transitivity

Proposition (Cameron & K, walking to lunch in Lisbon)

If Q is a finite simple nonassociative automorphic loop, then $Mlt(Q)$ is not 2-transitive.

Proof.

If $Inn(Q)$ is transitive on $Q \setminus \{1\}$, then all nonidentity elements of Q must have the same order since $Inn(Q)$ consists of automorphisms. This common order must be a prime p. Thus Q is a p-loop, hence not simple. □

A Basic Bound

Proposition (Cameron, email 3 Sept 2014)

If H and K are subgroups of $Mlt(Q)$ fixing h and k points respectively, with $H < K$ and $h > k > 0$, then $h \geq 2k$.

The reason is that the fixed points of a set of automorphisms of a loop form a subloop. But a subloop of a finite loop cannot have order more than half the order of the larger loop.

Basic Bounds II

Proposition (Cameron, July '14)

Let Q be an automorphic loop of order n. Then

$$|Mlt(Q)| \leq n^{1+\log_2 n}$$

Diagonal Type

Proposition

If $Mlt(Q)$ is of diagonal type. Then $Mlt(Q)$ has at most two factors.

Proof.

Suppose $Mlt(Q)$ has socle $N = T^k$ for some simple group T, and stabilizer $N_1 = \{(x, \dots, x) \mid x \in T\}$. N is characteristic, hence invariant under conjugation by $J : x \mapsto x^{-1}$. Thus J permutes the factors, say, $(T \times 1 \times \dots)^J = 1 \times T \times \dots$. Hence for each $x \in T$, $(x, 1, \dots)^J = (1, y, \dots)$ for some $y \in T$. But then if $u = (x, y, 1, \dots)$, we have $u^J = u$. Thus $u \in Inn(Q)$, hence $u \in N_1$. This is a contradiction if $k > 2$. □

Computer Search

Using the libraries of primitive groups in GAP and Magma, we now know…

Theorem

There are no finite nonassociative simple automorphic loops up to order

- 2500 *(Johnson, K, Nagý, Vojtěchovský '10)*
- 4096 *(Cameron & Leemans '15)*

Where Are We?

If Q is a finite simple nonassociative automorphic loop, then...

- Q is not commutative;
- $|Q| > 4096$, $|Q|$ is even and not a power of 2;
- $Mlt(Q)$ is primitive and nonsolvable;
- $Mlt(Q)$ cannot have regular socle, hence is neither of affine nor of twisted affine type;
- $Mlt(Q)$ is not 2-transitive;
- If $Mlt(Q)$ is of diagonal type, then there are at most two factors.

What do we **not** know?

Keep in mind that for finite (noncommutative) automorphic loops, we do not know...

Problem (Lagrange property)

Does the order of a subloop necessarily divide the order of the loop?

If every finite simple automorphic loop is a group, *then* the Lagrange property will hold.

(This is what happened for Moufang loops: the proof of the Lagrange property depends on the classification of finite simple Moufang loops, which in turn depends on CFSG.)

What's next?

A permutation group has (permutation) rank 3 if every point stabilizer has exactly 3 orbits.

If $Mlt(Q)$ is primitive and of rank 3, then within each of the two nontrivial orbits of $Inn(Q)$, all elements have the same order. It is easy to see one order must be 2, the other an odd prime p.

Hence every nonidentity element has order 2 or order p. This would be a very strange loop, but that's all we can say right now.

Thanks

Thank you!!!