In Memoriam

William Walker McCune

December 1953 - May 2011

Automorphic Loops

Petr Vojtěchovský

Department of Mathematics
University of Denver

July 25, 2011 / Loops '11, Czech Republic

Overview

1. Introduction

Overview

1. Introduction
2. Automorphic loops and associated operations

Overview

1. Introduction
2. Automorphic loops and associated operations
3. Odd Order Theorem for automorphic loops

Overview

Overview

Overview

Overview

Automorphic loops

For a loop Q define

$$
\begin{aligned}
L_x(y) &= xy\,, \qquad R_x(y) = yx\\
L_{x,y} &= L_{xy}^{-1}L_xL_y\,, \quad R_{x,y} = R_{xy}^{-1}R_yR_x\,, \quad T_x = R_x^{-1}L_x\\
\mathrm{Mlt}(Q) &= \langle L_x, R_x;\ x \in Q\rangle\\
\mathrm{Inn}(Q) &= (\mathrm{Mlt}(Q))_1 = \langle L_{x,y}, R_{x,y}, T_x;\ x, y \in Q\rangle\\
\mathrm{Aut}(Q) &= \text{ the automorphism group of } Q
\end{aligned}
$$

Automorphic loops

For a loop Q define

$$
\begin{aligned}
L_x(y) &= xy, \qquad R_x(y) = yx \\
L_{x,y} &= L_{xy}^{-1}L_xL_y, \quad R_{x,y} = R_{xy}^{-1}R_yR_x, \quad T_x = R_x^{-1}L_x \\
\mathrm{Mlt}(Q) &= \langle L_x, R_x;\ x \in Q\rangle \\
\mathrm{Inn}(Q) &= (\mathrm{Mlt}(Q))_1 = \langle L_{x,y}, R_{x,y}, T_x;\ x, y \in Q\rangle \\
\mathrm{Aut}(Q) &= \text{ the automorphism group of } Q
\end{aligned}
$$

Definition (Automorphic loops)

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

Automorphic loops

For a loop Q define

$$L_x(y) = xy, \qquad R_x(y) = yx$$
$$L_{x,y} = L_{xy}^{-1} L_x L_y, \quad R_{x,y} = R_{xy}^{-1} R_y R_x, \quad T_x = R_x^{-1} L_x$$
$$\mathrm{Mlt}(Q) = \langle L_x, R_x;\ x \in Q \rangle$$
$$\mathrm{Inn}(Q) = (\mathrm{Mlt}(Q))_1 = \langle L_{x,y}, R_{x,y}, T_x;\ x, y \in Q \rangle$$
$$\mathrm{Aut}(Q) = \text{ the automorphism group of } Q$$

Definition (Automorphic loops)

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

Groups and commutative Moufang loops are automorphic.

Equivalent definitions

The following definitions are equivalent:

1. Q is automorphic

Equivalent definitions

The following definitions are equivalent:

1. Q is automorphic
2. For every $x, y, u, v \in Q$

$$(xy)\backslash(x(yu)) \cdot (xy)\backslash(x(yv)) = (xy)\backslash(x(y(uv)))$$
$$((ux)y)/(xy) \cdot ((vx)y)/(xy) = (((uv)x)y)/(xy)$$
$$(xu)/x \cdot (xv)/x = (x(uv))/x$$

Equivalent definitions

The following definitions are equivalent:

1. Q is automorphic
2. For every $x, y, u, v \in Q$

$$(xy)\backslash(x(yu)) \cdot (xy)\backslash(x(yv)) = (xy)\backslash(x(y(uv)))$$
$$((ux)y)/(xy) \cdot ((vx)y)/(xy) = (((uv)x)y)/(xy)$$
$$(xu)/x \cdot (xv)/x = (x(uv))/x$$

3. For every $x \in Q$, $h \in \mathrm{Inn}(Q)$

$$hL_xh^{-1} = L_{h(x)}$$

(because $h(xh^{-1}(y)) = h(x)y$ iff $h(xy) = h(x)h(y)$)

Equivalent definitions

The following definitions are equivalent:

1. Q is automorphic
2. For every $x, y, u, v \in Q$

$$(xy)\backslash(x(yu)) \cdot (xy)\backslash(x(yv)) = (xy)\backslash(x(y(uv)))$$
$$((ux)y)/(xy) \cdot ((vx)y)/(xy) = (((uv)x)y)/(xy)$$
$$(xu)/x \cdot (xv)/x = (x(uv))/x$$

3. For every $x \in Q$, $h \in \mathrm{Inn}(Q)$

$$hL_xh^{-1} = L_{h(x)}$$

   (because $h(xh^{-1}(y)) = h(x)y$ iff $h(xy) = h(x)h(y)$)

4. $\mathrm{Inn}(Q) \subseteq N_{\mathrm{Mlt}(Q)}(\{L_x;\ x \in Q\})$

Equivalent definitions

The following definitions are equivalent:

1. Q is automorphic
2. For every $x, y, u, v \in Q$

$$(xy)\backslash(x(yu)) \cdot (xy)\backslash(x(yv)) = (xy)\backslash(x(y(uv)))$$
$$((ux)y)/(xy) \cdot ((vx)y)/(xy) = (((uv)x)y)/(xy)$$
$$(xu)/x \cdot (xv)/x = (x(uv))/x$$

3. For every $x \in Q$, $h \in \mathrm{Inn}(Q)$

$$hL_xh^{-1} = L_{h(x)}$$

(because $h(xh^{-1}(y)) = h(x)y$ iff $h(xy) = h(x)h(y)$)

4. $\mathrm{Inn}(Q) \subseteq N_{\mathrm{Mlt}(Q)}(\{L_x;\ x \in Q\})$
5. $\langle L_{x,y}, T_x;\ x, y \in Q\rangle \leq \mathrm{Aut}(Q)$

Chronology of results

1. 1956 Bruck and Paige
   basic properties

Chronology of results

1. 1956 Bruck and Paige
   basic properties
2. 1958 Osborn
   diassociative commutative A-loops are Moufang

Chronology of results

1. 1956 Bruck and Paige
   basic properties
2. 1958 Osborn
   diassociative commutative A-loops are Moufang
3. 1988 Shchukin
   on nilpotency class of Q and $\mathrm{Mlt}(Q)$

Chronology of results

1. 1956 Bruck and Paige
   basic properties
2. 1958 Osborn
   diassociative commutative A-loops are Moufang
3. 1988 Shchukin
   on nilpotency class of Q and $\mathrm{Mlt}(Q)$
4. 2002 Kinyon, Kunen, Phillips
   diassociative A-loops are Moufang

Chronology of results

1. 1956 Bruck and Paige
   basic properties
2. 1958 Osborn
   diassociative commutative A-loops are Moufang
3. 1988 Shchukin
   on nilpotency class of Q and $\mathrm{Mlt}(Q)$
4. 2002 Kinyon, Kunen, Phillips
   diassociative A-loops are Moufang
5. 2008 Drápal
   examples of order pq

Chronology of results

1. 1956 Bruck and Paige
   basic properties
2. 1958 Osborn
   diassociative commutative A-loops are Moufang
3. 1988 Shchukin
   on nilpotency class of Q and $\mathrm{Mlt}(Q)$
4. 2002 Kinyon, Kunen, Phillips
   diassociative A-loops are Moufang
5. 2008 Drápal
   examples of order pq
6. 2010 Jedlička, Kinyon, V
   basic structure of commutative A-loops

Chronology of results

1. 1956 Bruck and Paige
   basic properties
2. 1958 Osborn
   diassociative commutative A-loops are Moufang
3. 1988 Shchukin
   on nilpotency class of Q and $\mathrm{Mlt}(Q)$
4. 2002 Kinyon, Kunen, Phillips
   diassociative A-loops are Moufang
5. 2008 Drápal
   examples of order pq
6. 2010 Jedlička, Kinyon, V
   basic structure of commutative A-loops
7. 2011 Csörgő, Grishkov, Jedlička, Johnson, Kinyon, Kunen, Nagy, V
   solvability, nilpotency, toward classification

Basic properties

Let Q be an automorphic loop. Then:

1. Q is power-associative [BrPa]

Basic properties

Let Q be an automorphic loop. Then:

1. Q is power-associative [BrPa]
2. nuclei are normal in Q [BrPa]

Basic properties

Let Q be an automorphic loop. Then:

1. Q is power-associative [BrPa]
2. nuclei are normal in Q [BrPa]
3. $\mathrm{Nuc}_\ell(Q) \le \mathrm{Nuc}_m(Q)$, $\mathrm{Nuc}_r(Q) \le \mathrm{Nuc}_m(Q)$ [BrPa]

Basic properties

Let Q be an automorphic loop. Then:

1. Q is power-associative [BrPa]
2. nuclei are normal in Q [BrPa]
3. $\mathrm{Nuc}_\ell(Q) \leq \mathrm{Nuc}_m(Q)$, $\mathrm{Nuc}_r(Q) \leq \mathrm{Nuc}_m(Q)$ [BrPa]
4. Q has the AAIP, i.e., $(xy)^{-1} = y^{-1}x^{-1}$

Basic properties

Let Q be an automorphic loop. Then:

1. Q is power-associative [BrPa]
2. nuclei are normal in Q [BrPa]
3. $\mathrm{Nuc}_\ell(Q) \leq \mathrm{Nuc}_m(Q)$, $\mathrm{Nuc}_r(Q) \leq \mathrm{Nuc}_m(Q)$ [BrPa]
4. Q has the AAIP, i.e., $(xy)^{-1} = y^{-1}x^{-1}$
5. if A char Q then $A \trianglelefteq Q$

Basic properties

Let Q be an automorphic loop. Then:

1. Q is power-associative [BrPa]
2. nuclei are normal in Q [BrPa]
3. $\mathrm{Nuc}_\ell(Q) \le \mathrm{Nuc}_m(Q)$, $\mathrm{Nuc}_r(Q) \le \mathrm{Nuc}_m(Q)$ [BrPa]
4. Q has the AAIP, i.e., $(xy)^{-1} = y^{-1}x^{-1}$
5. if A char Q then $A \trianglelefteq Q$
6. if A char $B \trianglelefteq Q$ then $A \trianglelefteq Q$

Recent techniques

In recent works on A-loops, the following techniques were used:

1. associated operations (imitating Glauberman)

Recent techniques

In recent works on A-loops, the following techniques were used:

1. associated operations (imitating Glauberman)
2. Lie algebras constructed from loops (imitating Wright)

Recent techniques

In recent works on A-loops, the following techniques were used:

1. associated operations (imitating Glauberman)
2. Lie algebras constructed from loops (imitating Wright)
3. automated deduction (with McCune's Prover9)

Recent techniques

In recent works on A-loops, the following techniques were used:

1. associated operations (imitating Glauberman)
2. Lie algebras constructed from loops (imitating Wright)
3. automated deduction (with McCune's Prover9)
4. classification of primitive groups of small degrees

Recent techniques

In recent works on A-loops, the following techniques were used:

1. associated operations (imitating Glauberman)
2. Lie algebras constructed from loops (imitating Wright)
3. automated deduction (with McCune's Prover9)
4. classification of primitive groups of small degrees
5. explicit calculations within $\mathrm{Mlt}(Q)$ (using Drápal+Nagy's algorithm in LOOPS)

Recent techniques

In recent works on A-loops, the following techniques were used:

1. associated operations (imitating Glauberman)
2. Lie algebras constructed from loops (imitating Wright)
3. automated deduction (with McCune's Prover9)
4. classification of primitive groups of small degrees
5. explicit calculations within $\mathrm{Mlt}(Q)$ (using Drápal+Nagy's algorithm in LOOPS)
6. $\mathbb{Z}_p$-modules (for p-loops)

Recent techniques

In recent works on A-loops, the following techniques were used:

1. associated operations (imitating Glauberman)
2. Lie algebras constructed from loops (imitating Wright)
3. automated deduction (with McCune's Prover9)
4. classification of primitive groups of small degrees
5. explicit calculations within $\mathrm{Mlt}(Q)$ (using Drápal+Nagy's algorithm in LOOPS)
6. $\mathbb{Z}_p$-modules (for p-loops)
7. anisotropic subspaces over $\mathbb{F}_p$ (for p-loops)

Recent techniques

In recent works on A-loops, the following techniques were used:

1. associated operations (imitating Glauberman)
2. Lie algebras constructed from loops (imitating Wright)
3. automated deduction (with McCune's Prover9)
4. classification of primitive groups of small degrees
5. explicit calculations within $\mathrm{Mlt}(Q)$ (using Drápal+Nagy's algorithm in LOOPS)
6. $\mathbb{Z}_p$-modules (for p-loops)
7. anisotropic subspaces over $\mathbb{F}_p$ (for p-loops)
8. group transversals (by Csörgő)

Unique 2-divisibility and odd order

Definition

A groupoid Q is *uniquely 2-divisible*, if $x \mapsto x^2$ is a bijection of Q. The unique solution y to $y^2 = x$ will be denoted by $y = x^{1/2}$.

Unique 2-divisibility and odd order

Definition

A groupoid Q is *uniquely 2-divisible*, if $x \mapsto x^2$ is a bijection of Q. The unique solution y to $y^2 = x$ will be denoted by $y = x^{1/2}$.

Theorem

Let Q be a finite commutative loop. Then $|Q|$ is odd iff Q is uniquely 2-divisible.

Unique 2-divisibility and odd order

Definition

A groupoid Q is *uniquely 2-divisible*, if $x \mapsto x^2$ is a bijection of Q. The unique solution y to $y^2 = x$ will be denoted by $y = x^{1/2}$.

Theorem

Let Q be a finite commutative loop. Then $|Q|$ is odd iff Q is uniquely 2-divisible.

Theorem

A finite automorphic (or Moufang) loop has odd order iff it is uniquely 2-divisible.

Bruck loops

Definition (Bruck loops, K-loops)

A loop satisfying $x(y(xz)) = (x(yx))z$ and $(xy)^{-1} = x^{-1}y^{-1}$ is a *Bruck loop*.

Bruck loops are nearly automorphic-loops:

Bruck loops

Definition (Bruck loops, K-loops)

A loop satisfying $x(y(xz)) = (x(yx))z$ and $(xy)^{-1} = x^{-1}y^{-1}$ is a *Bruck loop*.

Bruck loops are nearly automorphic-loops:

Theorem (Funk, P. Nagy, Kreuzer, Goodaire, Robinson)

Every Bruck loop Q satisfies $\langle L_{x,y};\ x,y \in Q\rangle \leq \mathrm{Aut}(Q)$.

Bruck loops

Definition (Bruck loops, K-loops)

A loop satisfying $x(y(xz)) = (x(yx))z$ and $(xy)^{-1} = x^{-1}y^{-1}$ is a *Bruck loop*.

Bruck loops are nearly automorphic-loops:

Theorem (Funk, P. Nagy, Kreuzer, Goodaire, Robinson)

Every Bruck loop Q satisfies $\langle L_{x,y};\ x, y \in Q\rangle \le \mathrm{Aut}(Q)$.

Corollary

Commutative Bruck loops (i.e., commutative Moufang loops) are A-loops.

Bruck loops of odd order

Definition

A loop Q is *solvable* if there is a series $1 = Q_0 \trianglelefteq Q_1 \trianglelefteq \cdots \trianglelefteq Q_m = Q$ such that Q_{i+1}/Q_i is an abelian group for every i.

Glauberman proved many structural results for Bruck loops Q of odd order:

Bruck loops of odd order

Definition

A loop Q is *solvable* if there is a series $1 = Q_0 \trianglelefteq Q_1 \trianglelefteq \cdots \trianglelefteq Q_m = Q$ such that Q_{i+1}/Q_i is an abelian group for every i.

Glauberman proved many structural results for Bruck loops Q of odd order:

1. Q is uniquely 2-divisible

Bruck loops of odd order

Definition

A loop Q is *solvable* if there is a series $1 = Q_0 \trianglelefteq Q_1 \trianglelefteq \cdots \trianglelefteq Q_m = Q$ such that Q_{i+1}/Q_i is an abelian group for every i.

Glauberman proved many structural results for Bruck loops Q of odd order:

1. Q is uniquely 2-divisible
2. Cauchy Theorem, Lagrange Theorem, Sylow p-Theorem and Hall π-Theorem hold for Q

Bruck loops of odd order

Definition

A loop Q is *solvable* if there is a series $1 = Q_0 \trianglelefteq Q_1 \trianglelefteq \cdots \trianglelefteq Q_m = Q$ such that Q_{i+1}/Q_i is an abelian group for every i.

Glauberman proved many structural results for Bruck loops Q of odd order:

1. Q is uniquely 2-divisible
2. Cauchy Theorem, Lagrange Theorem, Sylow p-Theorem and Hall π-Theorem hold for Q
3. Q is solvable (the Odd Order Theorem)

Bruck loops of odd order

Definition

A loop Q is *solvable* if there is a series $1 = Q_0 \trianglelefteq Q_1 \trianglelefteq \cdots \trianglelefteq Q_m = Q$ such that Q_{i+1}/Q_i is an abelian group for every i.

Glauberman proved many structural results for Bruck loops Q of odd order:

1. Q is uniquely 2-divisible
2. Cauchy Theorem, Lagrange Theorem, Sylow p-Theorem and Hall π-Theorem hold for Q
3. Q is solvable (the Odd Order Theorem)

He then transferred these results to Moufang loops of odd order as follows:

Moufang loops of odd order

Let Q be a Moufang loop of odd order. For $x, y \in Q$ define

$$x \circ y = (xy^2x)^{1/2}.$$

Then $(Q, \circ)$ is a Bruck loop, and the orders of elements in $(Q, \cdot)$, $(Q, \circ)$ coincide.

We call $\circ$ and similar constructions the *associated operations*.

Twisted subgroups

Glauberman's idea works more generally.

Definition (Twisted subgroup)

Let G be a group and $T \subseteq G$ be such that $1 \in T$, $T^{-1} = T$, $xTx \subseteq T$ for every $x \in T$.

Twisted subgroups

Glauberman's idea works more generally.

Definition (Twisted subgroup)

Let G be a group and $T \subseteq G$ be such that $1 \in T$, $T^{-1} = T$, $xTx \subseteq T$ for every $x \in T$.

Theorem (Aschbacher, Foguel, Kinyon)

Let T be a uniquely 2-divisible twisted subgroup. Define

$$x \circ y = (xy^2x)^{1/2}.$$

Then $(T, \circ)$ is a Bruck loop and powers of elements of T coincide in the two operations.

Twisted subgroups in A-loops

For $x \in Q$ define

$$P_x = L_{x^{-1}}^{-1} R_x \in \mathrm{Mlt}(Q),$$
$$P_Q = \{P_x;\ x \in Q\}.$$

Theorem

Let Q be an automorphic loop. Then P_Q is a twisted subgroup of $\mathrm{Mlt}(Q)$, $P_{x^n} = (P_x)^n$, and

$$P_x P_y P_x = P_{P_x(y)} = P_{x^{-1}\backslash(yx)}.$$

If Q is also uniquely 2-divisible then

$$P_x \circ P_y = (P_x P_y^2 P_x)^{1/2} = P_{(x^{-1}\backslash(y^2 x))^{1/2}}.$$

Lagrange and Cauchy Theorems for A-loops

Theorem

Let Q be a uniquely 2-divisible A-loop. Then $x \mapsto P_x$ is a bijection $Q \to P_Q$, so

$$(Q, \circ), \quad x \circ y = (x^{-1} \backslash (y^2 x))^{1/2}$$

is a uniquely 2-divisible Bruck loop. Moreover, if $A \leq Q$ then $A \leq (Q, \circ)$.

Lagrange and Cauchy Theorems for A-loops

Theorem

Let Q be a uniquely 2-divisible A-loop. Then $x \mapsto P_x$ is a bijection $Q \to P_Q$, so

$$(Q, \circ), \quad x \circ y = (x^{-1} \backslash (y^2 x))^{1/2}$$

is a uniquely 2-divisible Bruck loop. Moreover, if $A \leq Q$ then $A \leq (Q, \circ)$.

Corollary

Lagrange and Cauchy Theorems hold for automorphic loops of odd order.

Partial subloop correspondence

The trouble is that there is no correspondence between subloops of Q and subloops of $(Q, \circ)$.

Theorem

Let Q be an A-loop of odd order. Then:

Partial subloop correspondence

The trouble is that there is no correspondence between subloops of Q and subloops of $(Q, \circ)$.

Theorem

Let Q be an A-loop of odd order. Then:

1. *if $A \leq Q$ then $A \leq (Q, \circ)$,*

Partial subloop correspondence

The trouble is that there is no correspondence between subloops of Q and subloops of $(Q, \circ)$.

Theorem

Let Q be an A-loop of odd order. Then:

1. *if $A \leq Q$ then $A \leq (Q, \circ)$,*
2. $\mathrm{Inn}(Q) \leq \mathrm{Aut}(Q) \leq \mathrm{Aut}(Q, \circ)$,

Partial subloop correspondence

The trouble is that there is no correspondence between subloops of Q and subloops of $(Q,\circ)$.

Theorem

Let Q be an A-loop of odd order. Then:

1. *if $A \le Q$ then $A \le (Q,\circ)$,*
2. $\mathrm{Inn}(Q) \le \mathrm{Aut}(Q) \le \mathrm{Aut}(Q,\circ)$,
3. *if $A \le (Q,\circ)$ then*

$$A \le Q \text{ iff } h(A) = A \text{ for every } h \in \mathrm{Inn}(Q;A),$$

Partial subloop correspondence

The trouble is that there is no correspondence between subloops of Q and subloops of $(Q,\circ)$.

Theorem

Let Q be an A-loop of odd order. Then:

1. *if $A \le Q$ then $A \le (Q,\circ)$,*
2. $\mathrm{Inn}(Q) \le \mathrm{Aut}(Q) \le \mathrm{Aut}(Q,\circ)$,
3. *if $A \le (Q,\circ)$ then*

$$A \le Q \text{ iff } h(A) = A \text{ for every } h \in \mathrm{Inn}(Q;A),$$

4. *if A char $(Q,\circ)$ then $A \trianglelefteq Q$.*

Linear loops

In 1967, C. R. B. Wright investigated the following construction:

Theorem

Let $(A, +, \cdot)$ be an algebra. Define $(A, \bullet)$ by

$$x \bullet y = x + y - x \cdot y.$$

Then $(A, \bullet)$ is a loop iff

$$y \mapsto y - xy,\ y \mapsto y - yx \text{ are bijections of } A. \qquad \text{(I)}$$

Linear loops

In 1967, C. R. B. Wright investigated the following construction:

Theorem

Let $(A,+,\cdot)$ be an algebra. Define $(A,\bullet)$ by

$$x \bullet y = x + y - x \cdot y.$$

Then $(A,\bullet)$ is a loop iff

$$y \mapsto y - xy,\ y \mapsto y - yx \text{ are bijections of } A. \tag{I}$$

Definition (Linear loops)

A loop $(A,\bullet)$ obtained from $(A,+,\cdot)$ satisfying (I) is called *linear*.

Lie rings

Definition (Lie rings)

Let $(L,+)$ be an abelian group, and $[.,.] : L \times L \to L$ a binary operation such that

Then $(L,+,[.,.])$ is a *Lie ring*.

Let $(L,+,[.,.])$ be a Lie ring. Then:

Lie rings

Definition (Lie rings)

Let $(L, +)$ be an abelian group, and $[.,.] : L \times L \to L$ a binary operation such that

1. $[x, y] = -[y, x]$ (alternating),

Then $(L, +, [.,.])$ is a *Lie ring*.

Let $(L, +, [.,.])$ be a Lie ring. Then:

Lie rings

Definition (Lie rings)

Let $(L, +)$ be an abelian group, and $[.,.] : L \times L \to L$ a binary operation such that

1. $[x, y] = -[y, x]$ (alternating),
2. $[x + y, z] = [x, z] + [y, z]$ (biadditive),

Then $(L, +, [.,.])$ is a *Lie ring*.

Let $(L, +, [.,.])$ be a Lie ring. Then:

Lie rings

Definition (Lie rings)

Let $(L, +)$ be an abelian group, and $[.,.] : L \times L \to L$ a binary operation such that

1. $[x, y] = -[y, x]$ (alternating),
2. $[x + y, z] = [x, z] + [y, z]$ (biadditive),
3. $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ (Jacobi).

Then $(L, +, [.,.])$ is a *Lie ring*.

Let $(L, +, [.,.])$ be a Lie ring. Then:

Lie rings

Definition (Lie rings)

Let $(L, +)$ be an abelian group, and $[.,.] : L \times L \to L$ a binary operation such that

1. $[x, y] = -[y, x]$ (alternating),
2. $[x + y, z] = [x, z] + [y, z]$ (biadditive),
3. $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ (Jacobi).

Then $(L, +, [.,.])$ is a *Lie ring*.

Let $(L, +, [.,.])$ be a Lie ring. Then:

1. $A \leq (L, +)$ such that $[A, L] \subseteq A$ is an *ideal*,

Lie rings

Definition (Lie rings)

Let $(L, +)$ be an abelian group, and $[.,.] : L \times L \to L$ a binary operation such that

1. $[x, y] = -[y, x]$ (alternating),
2. $[x + y, z] = [x, z] + [y, z]$ (biadditive),
3. $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ (Jacobi).

Then $(L, +, [.,.])$ is a *Lie ring*.

Let $(L, +, [.,.])$ be a Lie ring. Then:

1. $A \leq (L, +)$ such that $[A, L] \subseteq A$ is an *ideal*,
2. if $[L, L] = 0$ then L is *abelian*,

Lie rings

Definition (Lie rings)

Let $(L, +)$ be an abelian group, and $[.,.] : L \times L \to L$ a binary operation such that

1. $[x, y] = -[y, x]$ (alternating),
2. $[x + y, z] = [x, z] + [y, z]$ (biadditive),
3. $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ (Jacobi).

Then $(L, +, [.,.])$ is a *Lie ring*.

Let $(L, +, [.,.])$ be a Lie ring. Then:

1. $A \leq (L, +)$ such that $[A, L] \subseteq A$ is an *ideal*,
2. if $[L, L] = 0$ then L is *abelian*,
3. L is *simple* iff not abelian and no nontrivial ideals.

Two conditions

Let $(L, +, [., .])$ be a Lie ring. In addition to the condition (I), consider

$$[[x, z], [y, z]] = 0. \qquad \text{(II)}$$

Theorem

Let $(L, +, [., .])$ *be a Lie ring satisfying* (I) *and* (II). *Then* $(L, \bullet)$ *defined by* $x \bullet y = x + y - [x, y]$ *is an automorphic loop.*

Two conditions

Let $(L, +, [.,.])$ be a Lie ring. In addition to the condition (I), consider

$$[[x, z], [y, z]] = 0. \qquad \text{(II)}$$

Theorem

Let $(L, +, [.,.])$ be a Lie ring satisfying (I) and (II). Then $(L, \bullet)$ defined by $x \bullet y = x + y - [x, y]$ is an automorphic loop.

Theorem

*Let Q be an A-loop of odd order, and **suppose** that the Bruck loop $(Q, \circ)$ is an abelian group. Define*

$$[x, y] = x \circ y \circ (xy)^{-1}.$$

Then $L = (Q, \circ, [.,.])$ is a Lie ring satisfying (I) and (II). Subrings of L = subloops of Q. Ideals of L = normal subloops of Q.

Proof of Odd Order Theorem 1

Theorem (Odd Order Theorem for A-loops)

Let Q be an automorphic loop of odd order. Then Q is solvable.

Proof:

Proof of Odd Order Theorem 1

Theorem (Odd Order Theorem for A-loops)

Let Q be an automorphic loop of odd order. Then Q is solvable.

Proof:

- Q minimal counterexample, necessarily simple, not a group

Proof of Odd Order Theorem 1

Theorem (Odd Order Theorem for A-loops)

Let Q be an automorphic loop of odd order. Then Q is solvable.

Proof:

- Q minimal counterexample, necessarily simple, not a group
- $(Q, \circ)$ solvable (by Glauberman), so $A = (Q, \circ)' \neq Q$

Proof of Odd Order Theorem 1

Theorem (Odd Order Theorem for A-loops)

Let Q be an automorphic loop of odd order. Then Q is solvable.

Proof:

- Q minimal counterexample, necessarily simple, not a group
- $(Q, \circ)$ solvable (by Glauberman), so $A = (Q, \circ)' \neq Q$
- since A char $(Q, \circ)$, we have $A \trianglelefteq Q$, $A = 1$

Proof of Odd Order Theorem 1

Theorem (Odd Order Theorem for A-loops)

Let Q be an automorphic loop of odd order. Then Q is solvable.

Proof:

- Q minimal counterexample, necessarily simple, not a group
- $(Q, \circ)$ solvable (by Glauberman), so $A = (Q, \circ)' \neq Q$
- since A char $(Q, \circ)$, we have $A \trianglelefteq Q$, $A = 1$
- $(Q, \circ)$ is an abelian group

Proof of Odd Order Theorem 2

Fix a prime p dividing $|Q|$. Then:

- $B = \{x \in Q;\ x^p = 1\}$ char $(Q, \circ)$, so $B \trianglelefteq Q$

Proof of Odd Order Theorem 2

Fix a prime p dividing $|Q|$. Then:

- $B = \{x \in Q;\ x^p = 1\}$ char $(Q, \circ)$, so $B \trianglelefteq Q$
- by Cauchy, $B \neq 1$, thus $B = Q$

Proof of Odd Order Theorem 2

Fix a prime p dividing $|Q|$. Then:

- $B = \{x \in Q;\ x^p = 1\}$ char $(Q, \circ)$, so $B \trianglelefteq Q$
- by Cauchy, $B \neq 1$, thus $B = Q$
- $(Q, \circ)$ is an elementary abelian p-group

Proof of Odd Order Theorem 2

Fix a prime p dividing $|Q|$. Then:

- $B = \{x \in Q;\ x^p = 1\}$ char $(Q, \circ)$, so $B \trianglelefteq Q$
- by Cauchy, $B \neq 1$, thus $B = Q$
- $(Q, \circ)$ is an elementary abelian p-group
- define Lie ring $L = (Q, \circ, [.,.])$ as above

Proof of Odd Order Theorem 2

Fix a prime p dividing $|Q|$. Then:

- $B = \{x \in Q;\ x^p = 1\}$ char $(Q, \circ)$, so $B \trianglelefteq Q$
- by Cauchy, $B \neq 1$, thus $B = Q$
- $(Q, \circ)$ is an elementary abelian p-group
- define Lie ring $L = (Q, \circ, [.,.])$ as above
- L is a finite-dimensional algebra over $\mathbb{F}_p$

Proof of Odd Order Theorem 2

Fix a prime p dividing $|Q|$. Then:

- $B = \{x \in Q;\ x^p = 1\}$ char $(Q, \circ)$, so $B \trianglelefteq Q$
- by Cauchy, $B \neq 1$, thus $B = Q$
- $(Q, \circ)$ is an elementary abelian p-group
- define Lie ring $L = (Q, \circ, [.,.])$ as above
- L is a finite-dimensional algebra over $\mathbb{F}_p$
- Q is simple, so L has no nontrivial ideals

Proof of Odd Order Theorem 2

Fix a prime p dividing $|Q|$. Then:

- $B = \{x \in Q;\ x^p = 1\}$ char $(Q, \circ)$, so $B \trianglelefteq Q$
- by Cauchy, $B \neq 1$, thus $B = Q$
- $(Q, \circ)$ is an elementary abelian p-group
- define Lie ring $L = (Q, \circ, [.,.])$ as above
- L is a finite-dimensional algebra over $\mathbb{F}_p$
- Q is simple, so L has no nontrivial ideals
- if L is abelian then $0 = [Q, Q]$, $xy = x \circ y$, contradiction

Proof of Odd Order Theorem 2

Fix a prime p dividing $|Q|$. Then:

- $B = \{x \in Q;\ x^p = 1\}$ char $(Q, \circ)$, so $B \trianglelefteq Q$
- by Cauchy, $B \neq 1$, thus $B = Q$
- $(Q, \circ)$ is an elementary abelian p-group
- define Lie ring $L = (Q, \circ, [.,.])$ as above
- L is a finite-dimensional algebra over $\mathbb{F}_p$
- Q is simple, so L has no nontrivial ideals
- if L is abelian then $0 = [Q, Q]$, $xy = x \circ y$, contradiction
- else $Q = [Q, Q]$, and we finish as follows:

Proof of Odd Order Theorem 3

Theorem ("Crust of thin sandwich", Zelmanov, Kostrikin, 1990)

Let $(L, +, [.,.])$ be a Lie ring generated by finitely many elements a satisfying

$$[[x,a],a] = [[[y,a],x],a] = 0 \text{ for all } x, y.$$

Then L is nilpotent.

In our case we have $Q = [Q,Q]$, and one can check that each $a = [u,v]$ works.

Products of squares

What to do when $|Q|$ is even?

Theorem (Prover9)

Let Q be a commutative automorphic loop. Then $x^2y^2 = (x \diamond y)^2$, where

$$x \diamond y = ((xy)\backslash x \cdot (yx)\backslash y)^{-1}.$$

Products of squares

What to do when $|Q|$ is even?

Theorem (Prover9)

Let Q be a commutative automorphic loop. Then $x^2y^2 = (x \diamond y)^2$, where

$$x \diamond y = ((xy)\backslash x \cdot (yx)\backslash y)^{-1}.$$

Theorem

Let Q be a commutative automorphic loop. Then $(Q, \diamond)$ is power-associative, commutative, with powers as in $(Q, \cdot)$. If $|Q|$ is odd then $(Q, \diamond) \cong (Q, \cdot)$. If Q is of exponent two then $(Q, \diamond)$ is an elementary abelian 2-group.

Decomposition theorem

With the product of squares results at our disposal, we have:

Theorem (Decomposition Theorem)

Let Q be a finite commutative automorphic loop. Then $Q = K \times H$, where K consists of element of odd order, $|K|$ is odd, H consists of elements of order a power of 2, and $|H|$ is a power of two.

Unlike in the case of abelian groups, K does not necessarily decompose further into p-primary components. Drápal constructed counterexamples of order pq.

Consequences

Let Q be a finite commutative automorphic loop. Then we immediately get:

1. The Lagrange and Cauchy Theorems hold.

Consequences

Let Q be a finite commutative automorphic loop. Then we immediately get:

1. The Lagrange and Cauchy Theorems hold.
2. $|Q| = p^m$ iff every element of Q has order a power of p.

Consequences

Let Q be a finite commutative automorphic loop. Then we immediately get:

1. The Lagrange and Cauchy Theorems hold.
2. $|Q| = p^m$ iff every element of Q has order a power of p.
3. If Q is simple and nonassociative then Q has exponent 2 and $|Q| = 2^m$.

Consequences

Let Q be a finite commutative automorphic loop. Then we immediately get:

1. The Lagrange and Cauchy Theorems hold.
2. $|Q| = p^m$ iff every element of Q has order a power of p.
3. If Q is simple and nonassociative then Q has exponent 2 and $|Q| = 2^m$.

In fact, we will see that all finite commutative A-loops are solvable. But this will require another approach.

Definition

A permutation group G is *primitive* on X if it acts transitively on X and preserves no nontrivial partition of X (as blocks). The *degree* of G is the cardinality of X.

Definition

A permutation group G is *primitive* on X if it acts transitively on X and preserves no nontrivial partition of X (as blocks). The *degree* of G is the cardinality of X.

Theorem (Albert)

A loop Q is simple iff $\mathrm{Mlt}(Q)$ is primitive on Q.

Definition

A permutation group G is *primitive* on X if it acts transitively on X and preserves no nontrivial partition of X (as blocks). The *degree* of G is the cardinality of X.

Theorem (Albert)

A loop Q is simple iff $\mathrm{Mlt}(Q)$ is primitive on Q.

1. Primitive groups of degree $d < 2500$ (perhaps $d < 4096$) have been classified by Roney-Dougal and Holt.

Definition

A permutation group G is *primitive* on X if it acts transitively on X and preserves no nontrivial partition of X (as blocks). The *degree* of G is the cardinality of X.

Theorem (Albert)

A loop Q is simple iff $\mathrm{Mlt}(Q)$ is primitive on Q.

1. Primitive groups of degree $d < 2500$ (perhaps $d < 4096$) have been classified by Roney-Dougal and Holt.
2. Let $\mathrm{Soc}(G)$ be the normal subgroup generated by all minimal normal subgroups. If $\mathrm{Soc}(G)$ is abelian then G is a subgroup of an affine group - so called *affine type*.

Definition

A permutation group G is *primitive* on X if it acts transitively on X and preserves no nontrivial partition of X (as blocks). The *degree* of G is the cardinality of X.

Theorem (Albert)

A loop Q is simple iff $\mathrm{Mlt}(Q)$ is primitive on Q.

1. Primitive groups of degree $d < 2500$ (perhaps $d < 4096$) have been classified by Roney-Dougal and Holt.
2. Let $\mathrm{Soc}(G)$ be the normal subgroup generated by all minimal normal subgroups. If $\mathrm{Soc}(G)$ is abelian then G is a subgroup of an affine group - so called *affine type*.
3. Some structural info is available for primitive groups of non-affine type, on specific degrees.

Reduction to affine type

Theorem

Let Q be a simple automorphic 2-loop. Then $\mathrm{Mlt}(Q)$ is of affine type and Q is commutative.

Reduction to affine type

Theorem

Let Q be a simple automorphic 2-loop. Then $\mathrm{Mlt}(Q)$ is of affine type and Q is commutative.

Proof.

Reduction to affine case requires:

Commutativity in the affine case is relatively straightforward with AAIP. $\square$

Reduction to affine type

Theorem

Let Q be a simple automorphic 2-loop. Then $\mathrm{Mlt}(Q)$ is of affine type and Q is commutative.

Proof.

Reduction to affine case requires:

1. Guralnick and Saxl's classification of primitive permutation groups of degree 2^d

Commutativity in the affine case is relatively straightforward with AAIP. $\square$

Reduction to affine type

Theorem

Let Q be a simple automorphic 2-loop. Then $\mathrm{Mlt}(Q)$ is of affine type and Q is commutative.

Proof.

Reduction to affine case requires:

1. Guralnick and Saxl's classification of primitive permutation groups of degree 2^d
2. Drápal's result: If $\mathrm{Mlt}(Q) \leq P\Gamma L(2, F)$, F finite, $|F| \neq 3, 4$, then $\mathrm{Mlt}(Q) \cong Q$ is cyclic.

Commutativity in the affine case is relatively straightforward with AAIP. $\square$

Solvability of commutative A-loops

Let Q be a nonassociative finite simple commutative A-loop. We need an analog of the Bruck loop $(Q, \circ)$ in the general case.

1. By earlier results, Q is of order 2^n and exponent 2.

Solvability of commutative A-loops

Let Q be a nonassociative finite simple commutative A-loop. We need an analog of the Bruck loop $(Q,\circ)$ in the general case.

1. By earlier results, Q is of order 2^n and exponent 2.
2. By the above, $(U,+) = \mathrm{Soc}(\mathrm{Mlt}(Q))$ is an elementary abelian 2-group, regular.

Solvability of commutative A-loops

Let Q be a nonassociative finite simple commutative A-loop. We need an analog of the Bruck loop $(Q, \circ)$ in the general case.

1. By earlier results, Q is of order 2^n and exponent 2.
2. By the above, $(U, +) = \mathrm{Soc}(\mathrm{Mlt}(Q))$ is an elementary abelian 2-group, regular.
3. For $x \in Q$, factor uniquely $R_x = u_x h_x$, $u_x \in U$, $h_x \in \mathrm{Inn}(Q)$.

Solvability of commutative A-loops

Let Q be a nonassociative finite simple commutative A-loop. We need an analog of the Bruck loop $(Q,\circ)$ in the general case.

1. By earlier results, Q is of order 2^n and exponent 2.
2. By the above, $(U,+) = \mathrm{Soc}(\mathrm{Mlt}(Q))$ is an elementary abelian 2-group, regular.
3. For $x \in Q$, factor uniquely $R_x = u_x h_x$, $u_x \in U$, $h_x \in \mathrm{Inn}(Q)$.
4. Note $(U,\cdot) \cong Q$, $u \cdot v = u^{h_{v(1)}} + v$.

Solvability of commutative A-loops

Let Q be a nonassociative finite simple commutative A-loop. We need an analog of the Bruck loop $(Q, \circ)$ in the general case.

1. By earlier results, Q is of order 2^n and exponent 2.
2. By the above, $(U, +) = \mathrm{Soc}(\mathrm{Mlt}(Q))$ is an elementary abelian 2-group, regular.
3. For $x \in Q$, factor uniquely $R_x = u_x h_x$, $u_x \in U$, $h_x \in \mathrm{Inn}(Q)$.
4. Note $(U, \cdot) \cong Q$, $u \cdot v = u^{h_{v(1)}} + v$.
5. Define $(U, +, [.,.])$ by $[.,.] = u + v - u \cdot v$, a Lie algebra again.

Solvability of commutative A-loops

Let Q be a nonassociative finite simple commutative A-loop. We need an analog of the Bruck loop $(Q, \circ)$ in the general case.

1. By earlier results, Q is of order 2^n and exponent 2.
2. By the above, $(U, +) = \mathrm{Soc}(\mathrm{Mlt}(Q))$ is an elementary abelian 2-group, regular.
3. For $x \in Q$, factor uniquely $R_x = u_x h_x$, $u_x \in U$, $h_x \in \mathrm{Inn}(Q)$.
4. Note $(U, \cdot) \cong Q$, $u \cdot v = u^{h_{v(1)}} + v$.
5. Define $(U, +, [.,.])$ by $[.,.] = u + v - u \cdot v$, a Lie algebra again.
6. Finish as in the odd case.

Solvability of commutative A-loops

Let Q be a nonassociative finite simple commutative A-loop. We need an analog of the Bruck loop $(Q, \circ)$ in the general case.

1. By earlier results, Q is of order 2^n and exponent 2.
2. By the above, $(U, +) = \mathrm{Soc}(\mathrm{Mlt}(Q))$ is an elementary abelian 2-group, regular.
3. For $x \in Q$, factor uniquely $R_x = u_x h_x$, $u_x \in U$, $h_x \in \mathrm{Inn}(Q)$.
4. Note $(U, \cdot) \cong Q$, $u \cdot v = u^{h_{v(1)}} + v$.
5. Define $(U, +, [.,.])$ by $[.,.] = u + v - u \cdot v$, a Lie algebra again.
6. Finish as in the odd case.

Theorem

Finite commutative automorphic loops are solvable.

Searching for simple automorphic loops

If Q is simple then $\mathrm{Mlt}(Q)$ is primitive. Identify Q with $L_Q = \{L_x;\ x \in Q\} \subseteq \mathrm{Mlt}(Q)$.

How to find L_Q in a primitive group G acting on a set Q?

Searching for simple automorphic loops

If Q is simple then $\mathrm{Mlt}(Q)$ is primitive. Identify Q with $L_Q = \{L_x;\ x \in Q\} \subseteq \mathrm{Mlt}(Q)$.

How to find L_Q in a primitive group G acting on a set Q?

Theorem

Let Q be an automorphic loop, $G = \mathrm{Mlt}(Q)$, $H = \mathrm{Inn}(Q)$. Then:

Searching for simple automorphic loops

If Q is simple then $\mathrm{Mlt}(Q)$ is primitive. Identify Q with $L_Q = \{L_x;\ x \in Q\} \subseteq \mathrm{Mlt}(Q)$.

How to find L_Q in a primitive group G acting on a set Q?

Theorem

Let Q be an automorphic loop, $G = \mathrm{Mlt}(Q)$, $H = \mathrm{Inn}(Q)$. Then:

1. $hL_xh^{-1} = L_{h(x)}$ *for every* $h \in H$,

Searching for simple automorphic loops

If Q is simple then $\mathrm{Mlt}(Q)$ is primitive. Identify Q with $L_Q = \{L_x;\ x \in Q\} \subseteq \mathrm{Mlt}(Q)$.

How to find L_Q in a primitive group G acting on a set Q?

Theorem

Let Q be an automorphic loop, $G = \mathrm{Mlt}(Q)$, $H = \mathrm{Inn}(Q)$. Then:

1. $hL_xh^{-1} = L_{h(x)}$ *for every* $h \in H$,
2. $L_x \in C(H_x)$. *Proof:*

$$hL_x(y) = h(xy) = h(x)h(y) = xh(y) = L_xh(y)$$

Searching for simple automorphic loops

If Q is simple then $\mathrm{Mlt}(Q)$ is primitive. Identify Q with $L_Q = \{L_x;\ x \in Q\} \subseteq \mathrm{Mlt}(Q)$.

How to find L_Q in a primitive group G acting on a set Q?

Theorem

Let Q be an automorphic loop, $G = \mathrm{Mlt}(Q)$, $H = \mathrm{Inn}(Q)$. Then:

1. $hL_xh^{-1} = L_{h(x)}$ *for every* $h \in H$,
2. $L_x \in C(H_x)$. *Proof:*

$$hL_x(y) = h(xy) = h(x)h(y) = xh(y) = L_xh(y)$$

3. $\mathrm{Mlt}(Q)$ *is not 4-transitive,*

Searching for simple automorphic loops

If Q is simple then $\mathrm{Mlt}(Q)$ is primitive. Identify Q with $L_Q = \{L_x;\ x \in Q\} \subseteq \mathrm{Mlt}(Q)$.

How to find L_Q in a primitive group G acting on a set Q?

Theorem

Let Q be an automorphic loop, $G = \mathrm{Mlt}(Q)$, $H = \mathrm{Inn}(Q)$. Then:

1. $hL_xh^{-1} = L_{h(x)}$ *for every* $h \in H$,
2. $L_x \in C(H_x)$. *Proof:*

$$hL_x(y) = h(xy) = h(x)h(y) = xh(y) = L_xh(y)$$

3. $\mathrm{Mlt}(Q)$ *is not 4-transitive,*
4. *If Q is simple, $\mathrm{Mlt}(Q)$ is not solvable [Vesanen].*

Vainly searching for simple A-loops

This greatly speeds up the general purpose algorithm of Drápal and Nagy in the LOOPS package:

Algorithm

Let G be a transitive group on Q, $H = G_1$. Is there a loop Q such that $\mathrm{Mlt}(Q) \le G$, $\mathrm{Mlt}_\ell(Q) \le G$? (In the automorphic case, we also want $H \le \mathrm{Aut}(Q)$.)

The outcome:

Vainly searching for simple A-loops

This greatly speeds up the general purpose algorithm of Drápal and Nagy in the LOOPS package:

Algorithm

Let G be a transitive group on Q, $H = G_1$. Is there a loop Q such that $\mathrm{Mlt}(Q) \le G$, $\mathrm{Mlt}_\ell(Q) \le G$? (In the automorphic case, we also want $H \le \mathrm{Aut}(Q)$.)

The outcome:

Theorem

There is no nonassociative simple A-loop of order < 2500. There are many small nonassocitive simple loops Q with $\mathrm{Inn}_\ell(Q) \le \mathrm{Aut}(Q)$.

Automorphic p-loops

A consequence of the Cauchy and Lagrange Theorems:

Theorem

Let Q be a finite commutative automorphic loop and p a prime. Then $|Q| = p^k$ iff all elements of Q are p-elements.

So the concept of a p-loop is unambiguous, except possibly for $p = 2$ in the general case.

Automorphic p-loops

A consequence of the Cauchy and Lagrange Theorems:

Theorem

Let Q be a finite commutative automorphic loop and p a prime. Then $|Q| = p^k$ iff all elements of Q are p-elements.

Theorem

*Let Q be a finite automorphic loop and p an **odd** prime. Then $|Q| = p^k$ iff all elements of Q are p-elements.*

So the concept of a p-loop is unambiguous, except possibly for $p = 2$ in the general case.

Automorphic loops of order p^2

Theorem (Csörgő)

Let p be a prime. An A-loop of order p^2 is a group.

Automorphic loops of order p^2

Theorem (Csörgő)

Let p be a prime. An A-loop of order p^2 is a group.

Proof.

Original proof uses transversals and Odd Order Theorem. A quick proof:

$\square$

Automorphic loops of order p^2

Theorem (Csörgő)

Let p be a prime. An A-loop of order p^2 is a group.

Proof.

Original proof uses transversals and Odd Order Theorem. A quick proof:

1. enough to consider p odd

□

Automorphic loops of order p^2

Theorem (Csörgő)

Let p be a prime. An A-loop of order p^2 is a group.

Proof.

Original proof uses transversals and Odd Order Theorem. A quick proof:

1. enough to consider p odd
2. $(Q, \circ)$ is a Bruck loop of order p^2, hence abelian group

$\square$

Automorphic loops of order p^2

Theorem (Csörgő)

Let p be a prime. An A-loop of order p^2 is a group.

Proof.

Original proof uses transversals and Odd Order Theorem. A quick proof:

1. enough to consider p odd
2. $(Q, \circ)$ is a Bruck loop of order p^2, hence abelian group
3. the associated Lie ring is a Lie algebra over $\mathbb{F}_p$ of dimension two

$\square$

Automorphic loops of order p^2

Theorem (Csörgő)

Let p be a prime. An A-loop of order p^2 is a group.

Proof.

Original proof uses transversals and Odd Order Theorem. A quick proof:

1. enough to consider p odd
2. $(Q, \circ)$ is a Bruck loop of order p^2, hence abelian group
3. the associated Lie ring is a Lie algebra over $\mathbb{F}_p$ of dimension two
4. the only such algebra (classification) violates (I).

$\square$

Nilpotency in commutative automorphic p-loops

Definition

A loop Q is *(centrally) nilpotent* if Q, $Q/Z(Q)$, $(Q/Z(Q))/Z(Q/Z(Q))$, $\dots$, terminates with 1 in finitely many steps.

Recall that, for instance, Moufang p-loops are nilpotent. Using associated Bruck loops, we showed:

There is a commutative A-loop of order 8 with trivial center.

Nilpotency in commutative automorphic p-loops

Definition

A loop Q is *(centrally) nilpotent* if Q, $Q/Z(Q)$, $(Q/Z(Q))/Z(Q/Z(Q))$, $\dots$, terminates with 1 in finitely many steps.

Recall that, for instance, Moufang p-loops are nilpotent. Using associated Bruck loops, we showed:

Theorem

*Let Q be a finite commutative automorphic p-loop, p **odd**. Then Q is nilpotent.*

There is a commutative A-loop of order 8 with trivial center.

Commutative A-loops of order p^3

Theorem

For a prime p, there are precisely 7 commutative automorphic loops of order p^3 up to isomorphism.

Commutative A-loops of order p^3

Theorem

For a prime p, there are precisely 7 commutative automorphic loops of order p^3 up to isomorphism.

Proof.

$\square$

Commutative A-loops of order p^3

Theorem

For a prime p, there are precisely 7 commutative automorphic loops of order p^3 up to isomorphism.

Proof.

1. $p = 2$ by brute force, for $p > 2$ they are nilpotent

$\square$

Commutative A-loops of order p^3

Theorem

For a prime p, there are precisely 7 commutative automorphic loops of order p^3 up to isomorphism.

Proof.

1. $p = 2$ by brute force, for $p > 2$ they are nilpotent
2. describe free 2-generated nilpotent class two automorphic p-loop F_p, on $(\mathbb{Z}_p)^6$

□

Commutative A-loops of order p^3

Theorem

For a prime p, there are precisely 7 commutative automorphic loops of order p^3 up to isomorphism.

Proof.

1. $p = 2$ by brute force, for $p > 2$ they are nilpotent
2. describe free 2-generated nilpotent class two automorphic p-loop F_p, on $(\mathbb{Z}_p)^6$
3. $GL(2, p)$ acts on F_p

□

Commutative A-loops of order p^3

Theorem

For a prime p, there are precisely 7 commutative automorphic loops of order p^3 up to isomorphism.

Proof.

1. $p = 2$ by brute force, for $p > 2$ they are nilpotent
2. describe free 2-generated nilpotent class two automorphic p-loop F_p, on $(\mathbb{Z}_p)^6$
3. $GL(2, p)$ acts on F_p
4. orbits of the action on the Grassmannian of 3-dimensional subspaces of F_p = isom. classes of automorphic loops Q of order p^2 with $Z \leq Z(Q)$, $Z \cong \mathbb{Z}_p$, $Q/Z \cong \mathbb{Z}_p \times \mathbb{Z}_p$

□

Commutative A-loops of order p^3

Theorem

For a prime p, there are precisely 7 commutative automorphic loops of order p^3 up to isomorphism.

Proof.

1. $p = 2$ by brute force, for $p > 2$ they are nilpotent
2. describe free 2-generated nilpotent class two automorphic p-loop F_p, on $(\mathbb{Z}_p)^6$
3. $GL(2, p)$ acts on F_p
4. orbits of the action on the Grassmannian of 3-dimensional subspaces of F_p = isom. classes of automorphic loops Q of order p^2 with $Z \leq Z(Q)$, $Z \cong \mathbb{Z}_p$, $Q/Z \cong \mathbb{Z}_p \times \mathbb{Z}_p$
5. determine the orbits (different for $p = 3$)

$\square$

Anisotropic planes

Let F be a field and V a finite-dimensional vector space over F. Then $q: V \to F$ is a *quadratic form* if

$$q(\lambda u) = \lambda^2 q(u),$$
$$f(u,v) = q(u+v) - q(u) - q(v) \text{ is bilinear.}$$

Call $U \leq (V,q)$ *anisotropic* if $q(u) \neq 0$ for all $0 \neq u \in U$.

Theorem (see Scharlau for odd characteristic)

If F is finite and (V,q) is anisotropic, then $\dim(V) \leq 2$. All such subspaces of dimension two are isometric.

Anisotropic planes

Let F be a field and V a finite-dimensional vector space over F. Then $q : V \to F$ is a *quadratic form* if

$$q(\lambda u) = \lambda^2 q(u),$$
$$f(u, v) = q(u + v) - q(u) - q(v) \text{ is bilinear.}$$

Call $U \leq (V, q)$ *anisotropic* if $q(u) \neq 0$ for all $0 \neq u \in U$.

Theorem (see Scharlau for odd characteristic)

If F is finite and (V, q) is anisotropic, then $\dim(V) \leq 2$. All such subspaces of dimension two are isometric.

Theorem

For $A \in GL(2, F)$, $q = \det$, the plane $FI \oplus FA$ is anisotropic iff

$$\det(A - \lambda I) = \lambda^2 - \mathrm{tr}(A)\lambda + \det(A)$$

has no roots.

A-loops from anisotropic planes

Theorem

Let $F = \mathbb{F}_p$, $A \in GL(2,p)$ be such that $FI \oplus FA$ is anisotropic. Define $Q = Q(A)$ on $F \times (F \times F)$ by

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

Then Q is an A-loop of order p^3, exponent p, and $\mathrm{Nuc}_\ell(Q) = \mathrm{Nuc}_r(Q) = \mathrm{Nuc}(Q) = Z(Q) = 1$.

A-loops from anisotropic planes

Theorem

Let $F = \mathbb{F}_p$, $A \in GL(2,p)$ be such that $FI \oplus FA$ is anisotropic. Define $Q = Q(A)$ on $F \times (F \times F)$ by

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

Then Q is an A-loop of order p^3, exponent p, and $\mathrm{Nuc}_\ell(Q) = \mathrm{Nuc}_r(Q) = \mathrm{Nuc}(Q) = Z(Q) = 1$.

1. The condition "$FI \oplus FA$ anisotropic" is needed to get a quasigroup.

A-loops from anisotropic planes

Theorem

Let $F = \mathbb{F}_p$, $A \in GL(2,p)$ be such that $FI \oplus FA$ is anisotropic. Define $Q = Q(A)$ on $F \times (F \times F)$ by

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

Then Q is an A-loop of order p^3, exponent p, and $\mathrm{Nuc}_\ell(Q) = \mathrm{Nuc}_r(Q) = \mathrm{Nuc}(Q) = Z(Q) = 1$.

1. The condition "$FI \oplus FA$ anisotropic" is needed to get a quasigroup.
2. Can we find suitable A for every p?

Theorem

For every p there is $A \in GL(2, p)$ such that $FI \oplus FA$ is anisotropic.

Theorem

For every p there is $A \in GL(2,p)$ such that $FI \oplus FA$ is anisotropic.

Definition (Types)

Call $A \in GL(2,p)$ with $FI \oplus FA$ anisotropic of:

Theorem

For every p there is $A \in GL(2,p)$ such that $FI \oplus FA$ is anisotropic.

Definition (Types)

Call $A \in GL(2,p)$ with $FI \oplus FA$ anisotropic of:

1. *type 1* if $\mathrm{tr}(A) = 0$,

Theorem

For every p there is $A \in GL(2,p)$ such that $FI \oplus FA$ is anisotropic.

Definition (Types)

Call $A \in GL(2,p)$ with $FI \oplus FA$ anisotropic of:

1. *type 1* if $\mathrm{tr}(A) = 0$,
2. *type 2* if $\mathrm{tr}(A) \neq 0$ and $\det(A)$ is a quadratic residue,

Theorem

For every p there is $A \in GL(2,p)$ such that $FI \oplus FA$ is anisotropic.

Definition (Types)

Call $A \in GL(2,p)$ with $FI \oplus FA$ anisotropic of:

1. *type 1* if $\mathrm{tr}(A) = 0$,
2. *type 2* if $\mathrm{tr}(A) \neq 0$ and $\det(A)$ is a quadratic residue,
3. *type 3* if $\mathrm{tr}(A) \neq 0$ and $\det(A)$ is a quadratic nonresidue.

Theorem

For every p there is $A \in GL(2, p)$ such that $FI \oplus FA$ is anisotropic.

Definition (Types)

Call $A \in GL(2, p)$ with $FI \oplus FA$ anisotropic of:

1. *type 1* if $\mathrm{tr}(A) = 0$,
2. *type 2* if $\mathrm{tr}(A) \neq 0$ and $\det(A)$ is a quadratic residue,
3. *type 3* if $\mathrm{tr}(A) \neq 0$ and $\det(A)$ is a quadratic nonresidue.

It appears that the isomorphism type of $Q = Q(A)$ corresponds to the type of A. (Checked computationally for $p \leq 5$.)

Open problems

1. Is there a finite simple nonassociative A-loop?

Open problems

1. Is there a finite simple nonassociative A-loop?
2. Does $|x|$ divide $|Q|$ in noncommutative A-loops of even order?

Open problems

1. Is there a finite simple nonassociative A-loop?
2. Does $|x|$ divide $|Q|$ in noncommutative A-loops of even order?
3. Does Lagrange Theorem hold in noncommutative A-loops of even order?

Open problems

1. Is there a finite simple nonassociative A-loop?
2. Does $|x|$ divide $|Q|$ in noncommutative A-loops of even order?
3. Does Lagrange Theorem hold in noncommutative A-loops of even order?
4. Is “2-loop” well-defined for A-loops?

Open problems

1. Is there a finite simple nonassociative A-loop?
2. Does $|x|$ divide $|Q|$ in noncommutative A-loops of even order?
3. Does Lagrange Theorem hold in noncommutative A-loops of even order?
4. Is “2-loop” well-defined for A-loops?
5. Do Sylow p- and Hall π-Theorems hold in (commutative) A-loops?

Open problems

1. Is there a finite simple nonassociative A-loop?
2. Does $|x|$ divide $|Q|$ in noncommutative A-loops of even order?
3. Does Lagrange Theorem hold in noncommutative A-loops of even order?
4. Is “2-loop” well-defined for A-loops?
5. Do Sylow p- and Hall π-Theorems hold in (commutative) A-loops?
6. Classify A-loops of order p^3.

Open problems

1. Is there a finite simple nonassociative A-loop?
2. Does $|x|$ divide $|Q|$ in noncommutative A-loops of even order?
3. Does Lagrange Theorem hold in noncommutative A-loops of even order?
4. Is “2-loop” well-defined for A-loops?
5. Do Sylow p- and Hall π-Theorems hold in (commutative) A-loops?
6. Classify A-loops of order p^3.
7. Classify commutative A-loops of order p^4.

Open problems

1. Is there a finite simple nonassociative A-loop?
2. Does $|x|$ divide $|Q|$ in noncommutative A-loops of even order?
3. Does Lagrange Theorem hold in noncommutative A-loops of even order?
4. Is “2-loop” well-defined for A-loops?
5. Do Sylow p- and Hall π-Theorems hold in (commutative) A-loops?
6. Classify A-loops of order p^3.
7. Classify commutative A-loops of order p^4.
8. Classify A-loops of order pq.