Structure of commutative automorphic loops

Přemysl Jedlička[1], Michael K. Kinyon[2], Petr Vojtěchovský[2]

[1]Department of Mathematics
Faculty of Engineering (former Technical Faculty)
Czech University of Life Sciences (former Czech University of Agriculture), Prague

[2]Department of Mathematics
University of Denver

AAA 79, Olomouc
February 12, 2010

Quasigroups

Definition

Let $(G, \cdot)$ be a groupoid. The mapping $L_x : a \mapsto xa$ is called the *left translation* and the mapping $R_x : a \mapsto ax$ the right translation.

Definition (Combinatorial)

A groupoid $(Q, \cdot)$ is called a *quasigroup* if the mappings L_x and R_x are bijections, for each $x \in Q$.

Definition (Universal algebraic)

The algebra $(Q, \cdot, /, \backslash)$ is called a *quasigroup* if it satisfies the following identities:

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

Quasigroups

Definition

Let $(G, \cdot)$ be a groupoid. The mapping $L_x : a \mapsto xa$ is called the *left translation* and the mapping $R_x : a \mapsto ax$ the right translation.

Definition (Combinatorial)

A groupoid $(Q, \cdot)$ is called a *quasigroup* if the mappings L_x and R_x are bijections, for each $x \in Q$.

Definition (Universal algebraic)

The algebra $(Q, \cdot, /, \backslash)$ is called a *quasigroup* if it satisfies the following identities:

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

Loops

Definition

A quasigroup Q is called a *loop* if it contains the identity element.

Example (A minimal nonassociative loop)

	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

Multiplication Groups

Definitions

Let Q be a loop.

- The group generated by L_x and R_x, for all $x \in Q$, is called *the multiplication group* of Q and it is denoted by $\mathrm{Mlt}(Q)$.
- The subgroup of $\mathrm{Mlt}(Q)$ stabilizing the neutral element of Q is called *the inner mapping group* of Q and it is denoted by $\mathrm{Inn}(Q)$.

Fact

An inner mapping of a loop needs not to be an automorphism.

Definition

A loop Q is called an *automorphic loop* (or an *A-loop*) if $\mathrm{Inn}(Q) \leqslant \mathrm{Aut}(Q)$.

Multiplication Groups

Definitions

Let Q be a loop.

- The group generated by L_x and R_x, for all $x \in Q$, is called *the multiplication group* of Q and it is denoted by $\mathrm{Mlt}(Q)$.
- The subgroup of $\mathrm{Mlt}(Q)$ stabilizing the neutral element of Q is called *the inner mapping group* of Q and it is denoted by $\mathrm{Inn}(Q)$.

Fact

An inner mapping of a loop needs not to be an automorphism.

Definition

A loop Q is called an *automorphic loop* (or an *A-loop*) if $\mathrm{Inn}(Q) \leqslant \mathrm{Aut}(Q)$.

Multiplication Groups

Definitions

Let Q be a loop.

- The group generated by L_x and R_x, for all $x \in Q$, is called *the multiplication group* of Q and it is denoted by $\mathrm{Mlt}(Q)$.
- The subgroup of $\mathrm{Mlt}(Q)$ stabilizing the neutral element of Q is called *the inner mapping group* of Q and it is denoted by $\mathrm{Inn}(Q)$.

Fact

An inner mapping of a loop needs not to be an automorphism.

Definition

A loop Q is called an *automorphic loop* (or an *A-loop*) if $\mathrm{Inn}(Q) \leqslant \mathrm{Aut}(Q)$.

Multiplication Groups

Definitions

Let Q be a loop.

- The group generated by L_x and R_x, for all $x \in Q$, is called *the multiplication group* of Q and it is denoted by $\mathrm{Mlt}(Q)$.
- The subgroup of $\mathrm{Mlt}(Q)$ stabilizing the neutral element of Q is called *the inner mapping group* of Q and it is denoted by $\mathrm{Inn}(Q)$.

Fact

An inner mapping of a loop needs not to be an automorphism.

Definition

A loop Q is called an *automorphic loop* (or an *A-loop*) if $\mathrm{Inn}(Q) \leqslant \mathrm{Aut}(Q)$.

Multiplication Groups

Definitions

Let Q be a loop.

- The group generated by L_x and R_x, for all $x \in Q$, is called *the multiplication group* of Q and it is denoted by $\mathrm{Mlt}(Q)$.
- The subgroup of $\mathrm{Mlt}(Q)$ stabilizing the neutral element of Q is called *the inner mapping group* of Q and it is denoted by $\mathrm{Inn}(Q)$.

Fact

An inner mapping of a loop needs not to be an automorphism.

Definition

A loop Q is called an *automorphic loop* (or an *A-loop*) if $\mathrm{Inn}(Q) \leqslant \mathrm{Aut}(Q)$.

Basic properties of A-loops

Fact

Any characteristic subloop of an A-loop is normal.

Theorem (R. H. Bruck, J. L. Paige)

Every monogenerated subloop of an A-loop is a group.

Notation

We write x^3 instead of $x \cdot (x \cdot x)$ or $(x \cdot x) \cdot x$.
We write x^{-1} instead of $1/x$ or $x\backslash 1$.

Basic properties of A-loops

Fact

Any characteristic subloop of an A-loop is normal.

Theorem (R. H. Bruck, J. L. Paige)

Every monogenerated subloop of an A-loop is a group.

Notation

We write x^3 instead of $x \cdot (x \cdot x)$ or $(x \cdot x) \cdot x$.
We write x^{-1} instead of $1/x$ or $x\backslash 1$.

Basic properties of A-loops

Fact

Any characteristic subloop of an A-loop is normal.

Theorem (R. H. Bruck, J. L. Paige)

Every monogenerated subloop of an A-loop is a group.

Notation

We write x^3 instead of $x \cdot (x \cdot x)$ or $(x \cdot x) \cdot x$.
We write x^{-1} instead of $1/x$ or $x\backslash 1$.

Variety of A-loops

Fact

Let Q be a loop. The inner mapping group of Q is generated by the mappings

$$L_{xy}^{-1}L_xL_y, \qquad R_{xy}^{-1}R_xR_y \quad \text{and} \quad L_x^{-1}R_x,$$

where $x, y \in Q$.

Corollary

A loop is an A-loop iff it satisfies the following three identities:

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

Variety of A-loops

Fact

Let Q be a loop. The inner mapping group of Q is generated by the mappings

$$L_{xy}^{-1}L_xL_y, \qquad R_{xy}^{-1}R_xR_y \quad \text{and} \quad L_x^{-1}R_x,$$

where $x, y \in Q$.

Corollary

A loop is an A-loop iff it satisfies the following three identities:

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

Squares in Commutative A-loops

Question:

Do squares form a subloop of a commutative A-loop?

Lemma (P. J., M. K., P. V.)

$$x^2 \cdot y^2 = \Big(\big(x(x^2 \cdot y) \setminus (x^2 \cdot y) \big) / (x^2 \cdot y) \Big)^{-2}$$

Corollary (P. J., M. K., P. V.)

The set of all the squares forms a characteristic subloop of a commutative A-loop.

Squares in Commutative A-loops

Question:

Do squares form a subloop of a commutative A-loop?

Lemma (P. J., M. K., P. V.)

$$x^2 \cdot y^2 = \Big(\big(x(x^2 \cdot y) \setminus (x^2 \cdot y)\big)/(x^2 \cdot y)\Big)^{-2}$$

Corollary (P. J., M. K., P. V.)

The set of all the squares forms a characteristic subloop of a commutative A-loop.

Squares in Commutative A-loops

Question:

Do squares form a subloop of a commutative A-loop?

Lemma (P. J., M. K., P. V.)

$$x^2 \cdot y^2 = \Big(\big(x(x^2 \cdot y) \setminus (x^2 \cdot y) \big) / (x^2 \cdot y) \Big)^{-2}$$

$$x^2 \cdot y^2 = \big((xy \setminus x) \cdot (yx \setminus y) \big)^{-2}$$

Corollary (P. J., M. K., P. V.)

The set of all the squares forms a characteristic subloop of a commutative A-loop.

Squares in Commutative A-loops

Question:

Do squares form a subloop of a commutative A-loop?

Lemma (P. J., M. K., P. V.)

$$\cancel{x^2 \cdot y^2 = \Big(\big(x(x^2 \cdot y) \setminus (x^2 \cdot y) \big) / (x^2 \cdot y) \Big)^{-2}}$$

$$x^2 \cdot y^2 = \big((xy \setminus x) \cdot (yx \setminus y) \big)^{-2}$$

Corollary (P. J., M. K., P. V.)

The set of all the squares forms a characteristic subloop of a commutative A-loop.

Associated Loop

Definition

$$x \diamond y = \Big(\big(x(x^2 \cdot y) \setminus (x^2 \cdot y)\big) / (x^2 \cdot y) \Big)^{-1}$$

Proposition (P. J., M. K., P. V.)

Let Q be a commutative A-loop. Then $(Q, \diamond)$ is a commutative loop and powers in $(Q, \diamond)$ correspond to powers in $(Q, \cdot)$. Moreover, if $|Q|$ is odd then $(Q, \diamond) = (Q, \cdot)$.

Associated Loop

Definition

$$x \diamond y = \Big(\big(x(x^2 \cdot y) \setminus (x^2 \cdot y) \big) / (x^2 \cdot y) \Big)^{-1}$$

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

Proposition (P. J., M. K., P. V.)

Let Q be a commutative A-loop. Then $(Q, \diamond)$ is a commutative loop and powers in $(Q, \diamond)$ correspond to powers in $(Q, \cdot)$. Moreover, if $|Q|$ is odd then $(Q, \diamond) = (Q, \cdot)$.

Associated Loop

Definition

$$x \diamond y = \Big(\big(x(x^2 \cdot y) \backslash (x^2 \cdot y) \big) / (x^2 \cdot y) \Big)^{-1}$$

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

Proposition (P. J., M. K., P. V.)

Let Q be a commutative A-loop. Then $(Q, \diamond)$ is a commutative loop and powers in $(Q, \diamond)$ correspond to powers in $(Q, \cdot)$. Moreover, if $|Q|$ is odd then $(Q, \diamond) = (Q, \cdot)$.

Decomposition of Finite A-loops

Theorem (P. J., M. K., P. V.)

If Q is a finite commutative A-loop then $Q = K \times H$ where

$$K = \{x \in Q;\ |x| \text{ is odd}\},$$
$$H = \{x \in Q;\ x^{2^n} = 1,\ \text{ for an } n \in \mathbb{N}\}.$$

Moreover, $|K|$ is odd.

Idea of the proof.

We put

$$K = \bigcap_{n \geqslant 0} \{x^{2^n};\ x \in Q\} \quad \text{and} \quad H = \bigcup_{n \geqslant 0} \{x \in Q;\ x^{2^n} = 1\}.$$

□

Decomposition of Finite A-loops

Theorem (P. J., M. K., P. V.)

If Q is a finite commutative A-loop then $Q = K \times H$ where

$$K = \{x \in Q;\ |x| \text{ is odd}\},$$
$$H = \{x \in Q;\ x^{2^n} = 1, \ \text{ for an } n \in \mathbb{N}\}.$$

Moreover, $|K|$ is odd.

Idea of the proof.

We put

$$K = \bigcap_{n \geqslant 0} \{x^{2^n};\ x \in Q\} \quad \text{and} \quad H = \bigcup_{n \geqslant 0} \{x \in Q;\ x^{2^n} = 1\}.$$

□

Commutatives A-loops of odd orders

Proposition (P. J., M. K., P. V.)

Let $(Q, \cdot)$ be an commutative A-loop of an odd order. We associate to Q an operation $\circ$ defined as:

$$x \circ y = \sqrt{(x \cdot y^2)/x^{-1}}$$

Then Q is a Bruck loop. Moreover, the powers in $(Q, \cdot)$ coincide with the powers in $(Q, \circ)$

Corollary

- *Lagrange theorem,*
- *If $p \mid |Q|$, for p prime, then there exists $x \in Q$ of order p,*
- *Existence of Sylow p-subloops,*
- *Solvability.*

Commutatives A-loops of odd orders

Proposition (P. J., M. K., P. V.)

Let $(Q, \cdot)$ be an commutative A-loop of an odd order. We associate to Q an operation $\circ$ defined as:

$$x \circ y = \sqrt{(x \cdot y^2)/x^{-1}}$$

Then Q is a Bruck loop. Moreover, the powers in $(Q, \cdot)$ coincide with the powers in $(Q, \circ)$

Corollary

- *Lagrange theorem,*
- *If $p \mid |Q|$, for p prime, then there exists $x \in Q$ of order p,*
- *Existence of Sylow p-subloops,*
- *Solvability.*

Commutatives A-loops of odd orders

Proposition (P. J., M. K., P. V.)

Let $(Q, \cdot)$ be an commutative A-loop of an odd order. We associate to Q an operation $\circ$ defined as:

$$x \circ y = \sqrt{(x \cdot y^2)/x^{-1}}$$

Then Q is a Bruck loop. Moreover, the powers in $(Q, \cdot)$ coincide with the powers in $(Q, \circ)$

Corollary

- *Lagrange theorem,*
- *If $p \mid |Q|$, for p prime, then there exists $x \in Q$ of order p,*
- *Existence of Sylow p-subloops,*
- *Solvability.*

Commutatives A-loops of odd orders

Proposition (P. J., M. K., P. V.)

Let $(Q, \cdot)$ be an commutative A-loop of an odd order. We associate to Q an operation $\circ$ defined as:

$$x \circ y = \sqrt{(x \cdot y^2)/x^{-1}}$$

Then Q is a Bruck loop. Moreover, the powers in $(Q, \cdot)$ coincide with the powers in $(Q, \circ)$

Corollary

- *Lagrange theorem,*
- *If $p \mid |Q|$, for p prime, then there exists $x \in Q$ of order p,*
- *Existence of Sylow p-subloops,*
- *Solvability.*

Commutatives A-loops of odd orders

Proposition (P. J., M. K., P. V.)

Let $(Q, \cdot)$ be an commutative A-loop of an odd order. We associate to Q an operation $\circ$ defined as:

$$x \circ y = \sqrt{(x \cdot y^2)/x^{-1}}$$

Then Q is a Bruck loop. Moreover, the powers in $(Q, \cdot)$ coincide with the powers in $(Q, \circ)$

Corollary

- *Lagrange theorem,*
- *If $p \mid |Q|$, for p prime, then there exists $x \in Q$ of order p,*
- *Existence of Sylow p-subloops,*
- *Solvability.*

Commutatives A-loops of odd orders

Proposition (P. J., M. K., P. V.)

Let $(Q, \cdot)$ be an commutative A-loop of an odd order. We associate to Q an operation $\circ$ defined as:

$$x \circ y = \sqrt{(x \cdot y^2)/x^{-1}}$$

Then Q is a Bruck loop. Moreover, the powers in $(Q, \cdot)$ coincide with the powers in $(Q, \circ)$

Corollary

- *Lagrange theorem,*
- *If $p \mid |Q|$, for p prime, then there exists $x \in Q$ of order p,*
- *Existence of Sylow p-subloops,*
- *Solvability.*

Commutative A-loops of exponent 2

Proposition (P. J., M. K., P. V.)

Let Q be a commutative A-loop of exponent 2. Then $(Q, \diamond)$ is an elementary abelian group of exponent 2.

Corollary

Let Q be a finite commutative A-loop of exponent 2^k. Then $|Q| = 2^n$, for some n.

Theorem (P. J., M. K., P. V.)

Let Q be a finite commutative A-loop. Then

- *Q has the Lagrange property.*
- *Q has Sylow p-subloops, for each prime p dividing $|Q|$.*
- *Q has an element of order p, for such a p.*

Commutative A-loops of exponent 2

Proposition (P. J., M. K., P. V.)

Let Q be a commutative A-loop of exponent 2. Then $(Q, \diamond)$ is an elementary abelian group of exponent 2.

Corollary

Let Q be a finite commutative A-loop of exponent 2^k. Then $|Q| = 2^n$, for some n.

Theorem (P. J., M. K., P. V.)

Let Q be a finite commutative A-loop. Then

- *Q has the Lagrange property.*
- *Q has Sylow p-subloops, for each prime p dividing $|Q|$.*
- *Q has an element of order p, for such a p.*

Commutative A-loops of exponent 2

Proposition (P. J., M. K., P. V.)

Let Q be a commutative A-loop of exponent 2. Then $(Q, \diamond)$ is an elementary abelian group of exponent 2.

Corollary

Let Q be a finite commutative A-loop of exponent 2^k. Then $|Q| = 2^n$, for some n.

Theorem (P. J., M. K., P. V.)

Let Q be a finite commutative A-loop. Then

- *Q has the Lagrange property.*
- *Q has Sylow p-subloops, for each prime p dividing $|Q|$.*
- *Q has an element of order p, for such a p.*

Commutative A-loops of exponent 2

Proposition (P. J., M. K., P. V.)

Let Q be a commutative A-loop of exponent 2. Then $(Q, \diamond)$ is an elementary abelian group of exponent 2.

Corollary

Let Q be a finite commutative A-loop of exponent 2^k. Then $|Q| = 2^n$, for some n.

Theorem (P. J., M. K., P. V.)

Let Q be a finite commutative A-loop. Then

- *Q has the Lagrange property.*
- *Q has Sylow p-subloops, for each prime p dividing $|Q|$.*
- *Q has an element of order p, for such a p.*

Commutative A-loops of exponent 2

Proposition (P. J., M. K., P. V.)

Let Q be a commutative A-loop of exponent 2. Then $(Q,\diamond)$ is an elementary abelian group of exponent 2.

Corollary

Let Q be a finite commutative A-loop of exponent 2^k. Then $|Q| = 2^n$, for some n.

Theorem (P. J., M. K., P. V.)

Let Q be a finite commutative A-loop. Then

- *Q has the Lagrange property.*
- *Q has Sylow p-subloops, for each prime p dividing $|Q|$.*
- *Q has an element of order p, for such a p.*

Commutative A-loops of exponent 2

Proposition (P. J., M. K., P. V.)

Let Q be a commutative A-loop of exponent 2. Then $(Q, \diamond)$ is an elementary abelian group of exponent 2.

Corollary

Let Q be a finite commutative A-loop of exponent 2^k. Then $|Q| = 2^n$, for some n.

Theorem (P. J., M. K., P. V.)

Let Q be a finite commutative A-loop. Then

- *Q has the Lagrange property.*
- *Q has Sylow p-subloops, for each prime p dividing $|Q|$.*
- *Q has an element of order p, for such a p.*

Open Questions

Question:

Does there exist a (finite) non-solvable commutative A-loop?

Question:

Does there exist a (finite) simple non-cyclic commutative A-loop?

Question:

Does there exist a variety between abelian groups and commutative A-loops where

- each finite loop splits onto p-components,
- there exists a non-associative p-loop for each p.

Perhaps nilpotent commutative A-loops?

Open Questions

Question:

Does there exist a (finite) non-solvable commutative A-loop?

Question:

Does there exist a (finite) simple non-cyclic commutative A-loop?

Question:

Does there exist a variety between abelian groups and commutative A-loops where

- each finite loop splits onto p-components,
- there exists a non-associative p-loop for each p.

Perhaps nilpotent commutative A-loops?

Open Questions

Question:

Does there exist a (finite) non-solvable commutative A-loop?

Question:

Does there exist a (finite) simple non-cyclic commutative A-loop?

Question:

Does there exist a variety between abelian groups and commutative A-loops where

- each finite loop splits onto p-components,
- there exists a non-associative p-loop for each p.

Perhaps nilpotent commutative A-loops?

Open Questions

Question:

Does there exist a (finite) non-solvable commutative A-loop?

Question:

Does there exist a (finite) simple non-cyclic commutative A-loop?

Question:

Does there exist a variety between abelian groups and commutative A-loops where

- each finite loop splits onto p-components,
- there exists a non-associative p-loop for each p.

Perhaps nilpotent commutative A-loops?

References

- R. H. Bruck, J. L. Paige:
  Loops whose inner mappings are automorphisms,
  The Annals of Math., 2nd Series, **63**, no. 2, (1956), 308–323

- A. Drápal: A class of comm. loops with metacyclic inner mapping groups, Comment. Math. Univ. Carolin. **49**,3 (2008) 357–382.

- P. Jedlička, M. K. Kinyon, P. Vojtěchovský: Constructions of commutative automorphic loops, to appear in Comm. in Alg.

- P. Jedlička, M. K. Kinyon, P. Vojtěchovský: Structure of commutative automorphic loops, to appear in Trans. of AMS

- P. Jedlička, D. Simon: Commutative A-loops of order *pq* (preprint)

- M. K. Kinyon, K. Kunen, J. D. Phillips: Every diassociative A-loop is Moufang, Proc. Amer. Math. Soc. **130** (2002), 619–624

- M. K. Kinyon, K. Kunen, J. D. Phillips:
  Some notes on the structure of A-loops, (preprint)